# インストールと設定ガイド

## NetIQ Sentinel 7.0.1

**March 2012**

## 保証と著作権

NetIQ Corporation ( 以下「NetIQ」といいます ) は、オンラインヘルプまたはその他のドキュメントの内容またはそれらを使用した結果について、いかなる表明または保証も行っていません。また、オンラインヘルプまたはその他のドキュメントの商品性、および特定の目的への適合性について、明示と黙示を問わず一切保証しないものとします。NetIQ は、本書を改訂し、その内容をいつでも変更する権利を留保します。NetIQ は、このような改訂または変更に関し、いかなる個人または事業体に通知する義務を負いません。

NetIQ は、すべてのソフトウェアについて、いかなる表明または保証も行っていません。また、ソフトウェアの商品性、および特定の目的への適合性について、明示と黙示を問わず一切保証しないものとします。NetIQ は、NetIQ 製ソフトウェアの一部または全部を変更する権利を常に留保します。NetIQ は、このような変更に関し、いかなる個人または事業体に通知する義務を負いません。

本契約の下で提供される製品または技術情報はすべて、米国の輸出管理規定およびその他の国の輸出関連法規の制限を受けます。お客様は、すべての輸出規制を遵守して、製品の輸出、再輸出、または輸入に必要なすべての許可または等級を取得するものとします。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。NetIQ は、お客様が必要な輸出承認を取得しないことについては、いなかる責任も負わないものとします。



詳細については、NetIQ までお問い合わせください。お問い合わせ先は次のとおりです。

1233 West Loop South, Houston, Texas 77027

U.S.A

www.netiq.com

# 目次

# このガイドについて

このガイドでは NetIQ Sentinel について紹介し、Sentinel のインストール、移行、および設定の方法を説明します。

## 対象者

このガイドは、Sentinel 管理者およびコンサルタントを対象としています。

## フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインマニュアルの各ページの下部にあるユーザコメント機能を使用してください。

## マニュアルの更新

『*NetIQ Sentinel 7.0.1 インストールと設定ガイド*』の最新バージョンについては、Sentinel マニュアルの Web サイト (http://www.novell.com/documentation/sentinel70) を参照してください。

## その他のマニュアル

Sentinel テクニカルマニュアルは、次の分冊から構成されています。

- Sentinel 概要ガイド (http://www.novell.com/documentation/sentinel70/s70_overview/data/bookinfo.html)
- Sentinel クイックスタートガイド (http://www.novell.com/documentation/sentinel70/s70_quickstart/data/s70_quickstart.html)
- Sentinel 管理ガイド (http://www.novell.com/documentation/sentinel70/s70_admin/data/bookinfo.html)
- Sentinel ユーザガイド (http://www.novell.com/documentation/sentinel70/s70_user/data/bookinfo.html)
- Sentinel リンク概要ガイド (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html)
- Sentinel 内部監査イベント (http://www.novell.com/documentation/sentinel70/s70_auditevents/data/bookinfo.html)
- Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html)

  Sentinel SDK サイトには、ご自分のプラグインを構築するための情報が提供されています。

## Novell および NetIQ へのお問い合わせ

Sentinel は現在 NetIQ 製品ですが、Novell では引き続き製品サポートをしています。

- Novell Web サイト (http://www.novell.com)

- NetIQ Web サイト (http://www.netiq.com)
- 技術サポート (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- セルフサポート (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- パッチダウンロードサイト (http://download.novell.com/index.jsp)
- Sentinel コミュニティサポートフォーラム (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Sentinel TID (http://support.novell.com/products/sentinel)
- Sentinel プラグイン Web サイト (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- 電子メールお知らせリスト Sentinel プラグイン Web サイトから登録してください。

## セールスサポートへのお問い合わせ

商品、価格、機能についてのご質問は、ローカルパートナーへご連絡ください。ローカルパートナーとの連絡が取れない場合、セールスサポートチームへご連絡ください。

**各国共通 :** NetIQ 会社所在地 (http://www.netiq.com/about_netiq/officelocations.asp)

**米国およびカナダ :** 888-323-6768

**電子メール :** info@netiq.com

**Web サイト :** www.netiq.com

# インストール中

次の情報を使用して Sentinel をインストールします。

# 1 システム要件を満たす

以降のセクションでは、Sentinel のハードウェア、オペレーティングシステム、ブラウザ、サポートされるコネクタ、およびイベントソースの互換性の要件について説明します。



## 1.1 システム要件とサポートされるプラットフォーム

NetIQ は、以下に示すオペレーティングシステムでの Sentinel の運用をサポートします。また、これらのオペレーティングシステムにマイナーなアップデート ( セキュリティパッチやホットフィックスなど ) が適用されたシステムでも、Sentinel をサポートします。ただし、これらのオペレーティングシステムに対する主要な更新を搭載したシステムでの Sentinel の実行は、NetIQ がこれらの更新をテストおよび認定するまでサポートされません。



### 1.1.1 サポートされるオペレーティングシステムとプラットフォーム

次のオペレーティングシステムおよびプラットフォームにおいて、Sentinel サーバ、コレクタマネージャ、および相関エンジンがサポートされています。

| カテゴリ | 要件 |
| --- | --- |
| オペレーティングシステム | 次のオペレーティングシステムにおいて、Sentinel がサポートされています。<br>◆ SUSE Linux Enterprise Server (SLES) 11 SP1 64 ビット *<br>◆ Red Hat Enterprise Linux for Servers (RHEL) 6 64 ビット<br>* Sentinel 7 は、SLES の Open Enterprise Server インストールではサポートされません。 |
| 仮想プラットフォーム | NetIQ は、次の仮想プラットフォーム上に SLES 11 SP1 64 ビットサーバおよび Sentinel をインストールするアプライアンスを提供しています。<br>◆ VMWare ESX 4.0<br>◆ Xen 4.0 |
| DVD ISO | NetIQ は、以下のプラットフォーム上に SLES 11 SP1 64 ビットおよび Sentinel をインストールする DVD ISO ファイルを提供しています。<br>◆ Hyper-V Server 2008 R2<br>◆ オペレーティングシステムがインストールされていないハードウェア |

## 1.1.2 ハードウェア要件

Sentinel を実装するためのハードウェアの推奨事項は個々の実装によって異なるため、Sentinel のアーキテクチャを最終決定する前に、NetIQ コンサルティングサービスまたは NetIQ Sentinel パートナーにお問い合わせください。


- 12 ページの 「Sentinel サーバ」
- 13 ページの 「コレクタマネージャ」
- 14 ページの 「相関エンジン」


### Sentinel サーバ

このセクションでは、オンラインデータを 90 日間保持する運用システムのハードウェア推奨事項の一覧を示します。この推奨事項は、平均イベントサイズが 600 バイトであると想定したものです。ローカルストレージとネットワークストレージの推奨値には、実際のストレージ見積もりの 20% のバッファを持たせています。NetIQ は、見積もりが不正確だった場合や一部のサーバが時間の経過とともにビジーになる場合を考慮に入れて、バッファを取って構築することを推奨します。

1 台のサーバ上にすべての Sentinel コンポーネントがインストールされた状態で Sentinel サーバを実行する場合は、次のハードウェア推奨事項を考慮してください。

| カテゴリ | 100 EPS | 2500 EPS | 5000 EPS |
|---|---|---|---|
| CPU | Intel Xeon X5570 2.93-GHz (4 CPU コア ) x 1 | Intel Xeon X5470 3.33GHz (4 コア ) CPU x 2( 合計 8 コア ) | Intel Xeon X5470 3.33GHz (4 コア ) CPU x 2( 合計 8 コア ) |
| ローカルストレージ (30 日 ) | 2 x 256GB、7.2k RPM ドライブ ( ハードウェア RAID 1、256MB キャッシュ ) | 8 x 1.2TB、7.2k RPM ドライブ ( ハードウェア RAID 10、256MB キャッシュ ) | 16 x 1.2TB、15k RPM ドライブ ( ハードウェア RAID 10、512MB キャッシュ )、または同等のストレージエリアネットワーク (SAN) |
| ネットワークストレージ (90 日 ) | 2 x 128GB | 4 x 1TB | 8 x 1TB |
| Memory | **その他のインストール :**<br>4GB<br>**DVD ISO インストール :**<br>4.5GB | 16GB | 24GB |

**NOTE**: Sentinel は x86 64 ビット Intel Xeon および AMD Opteron プロセッサでサポートされていますが、Itanium などの純粋な 64 ビットプロセッサではサポートされていません。

最適なシステムパフォーマンスのためには、以下のガイドラインに従ってください。

- ローカルストレージには、イベントデータと生データの両方を含む、少なくとも 5 日分のデータを保持するのに十分な領域が必要です。データストレージの要件の計算の詳細については、16 ページのセクション 1.1.5「データストレージ要件の概算」を参照してください。
- ネットワークストレージには、ローカルストレージのイベントデータの完全に圧縮されたコピーを含めて、90 日分のデータが格納されます。検索およびレポーティングのパフォーマンス上の理由から、イベントデータのコピーがローカルストレージに保持されます。ストレージのコストが問題になる場合は、ローカルストレージのサイズを減らすことができます。ただし、圧縮解除のオーバーヘッドが生じるため、データをローカルストレージに置いた場合と比べて、検索およびレポートのパフォーマンスが約 70% 低下します。
- ネットワークストレージの場所は、外部の複数ドライブの SAN またはネットワーク接続ストレージ (NAS) に設定する必要があります。
- 推奨される、安定した状態のボリュームは、ライセンスされた最大 EPS の 80% です。この制限に達した場合、NetIQ は Sentinel インスタンスを追加することを推奨します。

## コレクタマネージャ

運用環境において、Sentinel サーバとは別のシステム上でコレクタマネージャを実行するには、次のハードウェア要件に従います。

| カテゴリ | 最小 | 推奨 |
|---|---|---|
| CPU | Intel Xeon L5240 3Ghz (2 コア ) | Intel Xeon X5570 2.93-GHz (4 CPU コア )×1 |
| Disk Space | 10GB (RAID 1) | 20GB (RAID 1) |
| Memory | 1.5GB | 4GB |
| 推定レート (EPS) | 500 | 2000 |

### 相関エンジン

運用環境において、Sentinel サーバとは別のシステム上で相関エンジンを実行するには、次のシステム要件に従います。

| カテゴリ | 最小 | 推奨 |
|---|---|---|
| CPU | Intel Xeon L5240 3Ghz (2 コア ) | Intel Xeon X5570 2.93-GHz (4 CPU コア )×1 |
| Disk Space | 10GB (RAID は不要です ) | 10GB (RAID は不要です ) |
| Memory | 1.5GB | 4GB |
| 推定レート (EPS) | 500 | 2500 |

## 1.1.3 サポートされるデータベースプラットフォーム

Sentinel には、埋め込みのファイルベースのストレージシステムおよびデータベースが含まれており、すべて Sentinel の実行に必要です。ただし、オプションのデータ同期機能を使用してデータをデータウェアハウスにコピーする場合、Sentinel では Oracle バージョン 11g R2 または Microsoft SQL Server 2008 R2 のデータウェアハウスとしての使用がサポートされています。

## 1.1.4 対応ブラウザ

Sentinel の Web インタフェースは、次の対応ブラウザを使用した、1280 x 1024 以上の解像度での表示用に最適化されています。

**NOTE**: Sentinel クライアントアプリケーションを正しくロードするには、システムに Sun Java プラグインがインストールされている必要があります。

| プラットフォーム | ブラウザ |
| --- | --- |
| Windows 7 | ◆ Firefox 5、6、7、8、9、および 10<br>◆ Internet Explorer 8 および 9 *<br><br>Internet Explorer 8 については、15 ページの 「Internet Explorer の前提条件」を参照してください。 |
| SLES 11 SP1 および RHEL 6 | ◆ Firefox 5、6、7、8、9、および 10<br><br>詳細については、15 ページの 「手動で Firefox のバージョンをアップデートする」を参照してください。 |

## Internet Explorer の前提条件

インターネットの［セキュリティのレベル］が［高］に設定されている場合、Sentinel にログインしても、ファイルダウンロードのポップアップがブラウザによってブロックされることがあります。この問題を回避するには、次のようにしてセキュリティのレベルをいったん［中高］に設定した後、［カスタム］レベルに変更してください。

1. *［ツール］* > *［インターネットオプション］* > *［セキュリティ］* の順にクリックし、セキュリティのレベルを *［中高］* に設定します。
2. *［ツール］* > *［互換表示］* オプションが選択されていないことを確認します。
3. *［ツール］* > *［インターネットオプション］* > *［セキュリティ］タブ* > *［レベルのカスタマイズ］* の順にクリックし、*［ダウンロード］* セクションまで下にスクロールし、*［ファイルのダウンロード時に自動的にダイアログを表示］* オプションの *［有効にする］* を選択します。

## 手動で Firefox のバージョンをアップデートする

Sentinel は Firefox のバージョン 5 から 10 までをサポートしていますが、SLES 11 SP1 システムにパッケージされているのは、Firefox バージョン 3.6*x* です。サポートされているバージョンの Firefox を組み込むために SLES 11 SP1 のインストールを手動で更新するには、次の手順を実行してください。

1. YaST を開きます。
2. ［*ソフトウェア*］> ［*ソフトウェアリポジトリ*］を選択して［設定されたソフトウェアリポジトリ］ウィンドウを表示します。
3. ［*追加*］をクリックして［メディアタイプ］ウィンドウを開きます。
4. ［*URL の指定*］オプションを選択してから、［*次へ*］をクリックします。

   これにより、［リポジトリ URL］ウィンドウが表示されます。
5. URL テキストボックスにソフトウェアリポジトリ (http://download.opensuse.org/repositories/mozilla/SLE_11/) のリンクを入力してから、［*次へ*］をクリックします。

   ソフトウェアリポジトリがダウンロードされます。
6. ［*OK*］をクリックしてソフトウェアリポジトリを更新します。
7. ［*ソフトウェア管理*］をクリックして［YaST2］ウィンドウを開きます。
8. ［*検索*］テキストボックスに「Firefox」と入力します。

Firefox パッケージのリストが表示されます。

9 インストールする Firefox に必要な、サポート対象バージョンのパッケージを選択します。

既存のバージョンと競合するパッケージを選択すると、［警告］ダイアログボックスが表示されます。該当するオプションを選択してから、［*了解 -- 再試行*］ボタンをクリックします。

10 ［*承諾*］をクリックします。

## 1.1.5 データストレージ要件の概算

Sentinel では、法令やその他の要件に従って、生データを長期間保持することができます。生データを圧縮することで、ローカルストレージやネットワークストレージのスペースを有効利用できます。それでも、時間が経過するにつれ、ストレージ必要量が大幅に増加する場合もあります。

予算に制約のある大規模なストレージシステムでは、データの長期保存には、コスト効果の高いデータストレージシステムを使用する必要があります。コスト効率の高さで言えば、第一に挙げられるのがテープベースのストレージシステムです。ただし、テープの場合、データへのランダムアクセスが不可能なため、高速検索は望めません。そのため、データを長期間にわたって保存する場合には、複数の手法を組み合わせて使用することが望ましいと言えます。つまり、検索する必要があるデータはランダムアクセスストレージシステムに保存し、保持する必要はあっても検索する必要のないデータは、テープなどのコスト効果の高いストレージに格納します。この複数の手法の組み合わせを使用する方法については、『*NetIQ Sentinel 7.0.1 管理ガイド*』の「「Using Sequential-Access Storage for Long Term Data Storage ( データの長期保存のために順次アクセスストレージを使用する )」」を参照してください。

Sentinel に必要なランダムアクセスストレージの容量を確認するには、何日間のデータに対して定期的な検索またはレポートを実行する必要があるかを最初に見積もります。Sentinel でデータのアーカイブに使用するための、十分な容量のあるハードドライブを用意する必要があります。そのためには、ローカルの Sentinel マシンを使用することも、Server Message Block (SMB) プロトコル、CIFS プロトコル、Network File System (NFS)、または SAN を使用してリモートのドライブに接続することもできます。

また、最低要件の容量に加えて、次に示すハードドライブの容量も必要になります。

- データの量が想定外に増えた場合を考慮して追加しておく容量。
- 古いデータの検索およびレポーティングを実行するために、Sentinel とテープとの間でデータをコピーするための容量。

次の計算式を使用してデータの保存に必要な容量を見積もります。

- **ローカルイベントストレージ ( 部分的に圧縮 ):** { イベント 1 件あたりの平均バイトサイズ } x { 日数 } x {1 秒間のイベント数 } x 0.00008 = 必要なストレージの合計 GB

  イベントサイズは、通常、300 ～ 1000 バイトです。
- **ネットワークイベントストレージ ( 完全に圧縮 ):** { イベント 1 件あたりの平均バイトサイズ } x { 日数 } x {1 秒間のイベント数 } x 0.00001 = 必要なストレージの合計 GB
- **生データストレージ ( ローカルストレージとネットワークストレージの両方で完全に圧縮 ):** { 生データレコード 1 件あたりの平均バイトサイズ } x { 日数 } x {1 秒間のイベント数 } x 0.000003 = 必要なストレージの合計 GB

  Syslog メッセージの平均的な生データのサイズは 200 バイトです。

- **合計ローカルストレージサイズ ( ネットワークストレージが有効な場合 ):** { 目的とする日数のローカルイベントストレージサイズ } + {1 日分の生データストレージサイズ } = 必要なストレージの合計 GB

  ネットワークストレージが使用可能になっている場合、イベントデータは平均しておよそ 2 日後にネットワークストレージにコピーされます。詳細については、『*NetIQ Sentinel 7.0.1 管理ガイド)*』の「「Configuring Data Storage ( データストレージの設定 )」」を参照してください。
- **合計ローカルストレージサイズ ( ネットワークストレージが無効な場合 ):** { 保持期間のローカルイベントストレージサイズ } + { 保持期間の生データストレージサイズ ) = 必要なストレージの合計 GB
- **合計ネットワークストレージサイズ :** { 保持期間のネットワークイベントストレージサイズ } + { 保持期間の生データストレージサイズ ) = 必要なストレージの合計 GB

---

**NOTE**:

- 各数式表現での係数 ((1 日の秒数 ) x (1 日の GB 数 ) x 圧縮比 )。
- これらの値はあくまでも概算であり、イベントデータのサイズや圧縮データのサイズによって異なります。
- 部分的に圧縮とは、データは圧縮されていますが、データのインデックスは圧縮されていないことを意味します。完全に圧縮とは、イベントデータとインデックスデータの両方が圧縮されていることを意味します。通常、イベントデータの圧縮比は 10:1 です。通常、インデックスの圧縮比は 5:1 です。インデックスは、データの検索を効率化するために使用されます。

---

また、上の計算式を使用して、テープなどの長期間にわたって使用されるデータストレージシステムに必要なストレージ容量を算出することもできます。

### 1.1.6 ディスク I/O 使用率の見積もり

サーバでのディスク使用量をさまざまな EPS レートで見積もるには、次の計算式を使用します。

- **ディスクに書き込まれるデータ ( キロバイト / 秒 ):** ( バイト単位の平均イベントサイズ + バイト単位の平均生データサイズ ) x (1 秒間のイベント数 ) x 圧縮係数 0.002 = 1 秒間にディスクに書き込まれるデータ

  たとえば、500EPS で、平均イベントサイズが 758 バイト、ログファイルの平均生データサイズが 490 バイトの場合は、ディスクに書き込まれるデータは次のようにして求められます。

  (758 バイト + 490 バイト ) x 500EPS x 0.002 = 1100KB
- **ディスクに対する I/O 要求の数 (1 秒間の転送数 ):** ( バイト単位の平均イベントサイズ + バイト単位の平均生データサイズ ) x (1 秒間のイベント数 ) x 圧縮係数 0.00002 = 1 秒間のディスクへの I/O 要求

  たとえば、500EPS で、平均イベントサイズが 758 バイト、ログファイルの平均生データサイズが 490 バイトの場合は、1 秒間のディスクへの I/O 要求数は次のようにして求められます。

  (758 バイト + 490 バイト ) x 500EPS x 0.00002 = 10 転送 / 秒
- **1 秒間にディスクに書き込まれるブロック数 :** ( バイト単位の平均イベントサイズ + バイト単位の平均生データサイズ ) x (1 秒間のイベント数 ) x 圧縮係数 0.003 = 1 秒間にディスクに書き込まれるブロック数

たとえば、500EPS で、平均イベントサイズが 758 バイト、ログファイルの平均生データサイズが 490 バイトの場合は、1 秒間にディスクに書き込まれるブロック数は次のようにして求められます。

(758 バイト + 490 バイト ) x 500EPS x 0.003 = 1800 ブロック / 秒

- **検索実行時にディスクから 1 秒間に読み込まれるデータ :** ( バイト単位の平均イベントサイズ + バイト単位の平均生データサイズ ) x ( クエリに一致するイベントの数 ( 百万単位 )) x 圧縮係数 0.40 = ディスクから 1 秒間に読み取られるキロバイト数

  たとえば、500 万のイベントが検索クエリに一致し、平均イベントサイズが 758 バイト、ログファイルの平均生データサイズが 490 バイトの場合は、1 秒間にディスクから読み取られるデータは次のようにして求められます。

  (758 バイト + 490 バイト ) x 5 x 0.40 = 500KB

### 1.1.7 ネットワーク帯域幅使用率の見積もり

次の計算式を使用して、Sentinel サーバとリモートコレクタマネージャの間でのネットワーク帯域幅の使用率を見積もります。

{ バイト単位の平均イベントサイズ + バイト単位の平均生データサイズ } x {1 秒間のイベント数 } x 圧縮係数 0.0003 = Kbps ( キロバイト / 秒 ) 単位のネットワーク帯域幅

たとえば、500EPS で、平均イベントサイズが 758 バイト、ログファイルの平均生データサイズが 490 バイトの場合は、ネットワーク帯域幅の使用率は次のようにして求められます。

(758 バイト + 490 バイト ) x 500EPS x .0003 = 175Kbps

### 1.1.8 仮想環境

Sentinel は、広範にわたるテストが実施されており、VMware ESX サーバで完全にサポートされています。仮想環境を設定する場合、仮想マシンには CPU が少なくとも 2 基必要です。ESX 上の物理マシンまたはその他の仮想環境におけるテストの結果と同等のパフォーマンス結果を達成するには、仮想環境が物理マシンで推奨される内容と同じメモリ、CPU、ディスク容量、および I/O を備える必要があります。

物理マシンで推奨される内容については、11 ページのセクション 1.1「システム要件とサポートされるプラットフォーム」を参照してください。

## 1.2 コネクタおよびコレクタのシステム要件

各コネクタおよびコレクタには、それぞれ独自のシステム要件およびサポートされるプラットフォームがあります。Sentinel プラグインの Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) にある、コネクタおよびコレクタのマニュアルを参照してください。

# 1.3 使用するポート



## 1.3.1 Sentinel サーバ

### ローカルポート

Sentinel は、データベースや他の内部プロセスとの内部通信に次のポートを使用します。

| ポート | 説明 |
|---|---|
| TCP 5432 | PostgreSQL データベースで使用されます。デフォルトでこのポートを開く必要はありません。ただし、Sentinel SDK を使用してレポートを作成する場合には、このポートを開く必要があります。詳細については、Sentinel プラグイン SDK の Web サイト (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) を参照してください。 |
| TCP 27017 | セキュリティインテリジェンス環境設定データベースで使用されます。 |
| TCP 28017 | セキュリティインテリジェンスデータベースの Web インタフェースで使用されます。 |
| TCP 32000 | ラッパープロセスとサーバプロセス間の内部通信で使用されます。 |

### ネットワークポート

Sentinel は、他のコンポーネントとの外部通信には異なるポートを使用します。アプライアンスをインストールするため、ポートはファイアウォール上でデフォルトで開かれています。ただし、標準的なインストールでは、Sentinel をインストールするオペレーティングシステム上で設定を行い、ファイアウォール上でポートを開く必要があります。

Sentinel が正常に動作するよう、次のポートがファイアウォール上で開かれていることを確認してください。

| ポート | 説明 |
| --- | --- |
| TCP 1099 および 2000 | 監視ツールが Java Management Extensions (JMX) を利用して Sentinel サーバプロセスに接続するのに使用されます。 |
| TCP 1289 | Audit の接続用に使用されます。 |
| UDP 1514 | Syslog メッセージ用に使用されます。 |
| TCP 8443 | HTTPS 通信に使用されます。 |
| TCP 1443 | SSL で暗号化された Syslog メッセージに使用されます。 |
| TCP 61616 | コレクタマネージャとサーバ間の通信に使用されます。 |
| TCP 10013 | Sentinel コントロールセンターおよびソリューションデザイナが使用します。 |
| TCP 1468 | Syslog メッセージ用に使用されます。 |
| TCP 10014 | リモートのコレクタマネージャにより、SSL プロキシを介してサーバに接続するのに使用されます。ただし、これは一般的ではありません。デフォルトでは、リモートのコレクタマネージャは SSL ポート 61616 を使用してサーバに接続します。 |

### Sentinel サーバアプライアンス固有のポート

Sentinel サーバアプライアンスでは、上記のポートに加えて次のポートが開いています。

| ポート | 説明 |
| --- | --- |
| TCP 22 | シェルが Sentinel アプライアンスに安全にアクセスできるようにするために使用されます。 |
| TCP 54984 | Sentinel アプライアンスの管理コンソール (WebYaST) で使用されます。Sentinel アプライアンスのアップデートサービスにも使用されます。 |
| TCP 289 | Audit の接続用に 1289 に転送されます。 |
| UDP 443 | HTTPS 通信用に 8443 に転送されます。 |
| UDP 514 | Syslog メッセージ用に 1514 に転送されます。 |
| TCP 1290 | SuSE Firewall を介した接続が許可される Sentinel リンクポートです。 |
| UDP および TCP 40000 - 41000 | syslog などのデータ収集サーバの設定に使用可能なポートです。Sentinel は、これらのポートをデフォルトではリスンしません。 |

## 1.3.2 コレクタマネージャ

### ネットワークポート

Sentinel コレクタマネージャが正常に動作できるよう、ファイアウォール上で次のポートが開かれていることを確認してください。

| ポート | 説明 |
| --- | --- |
| TCP 1289 | Audit の接続用に使用されます。 |
| UDP 1514 | Syslog メッセージ用に使用されます。 |
| TCP 1443 | SSL で暗号化された Syslog メッセージに使用されます。 |
| TCP 1468 | Syslog メッセージ用に使用されます。 |
| TCP 1099 および 2000 | 監視ツールが Java Management Extensions (JMX) を利用して Sentinel サーバプロセスに接続するのに使用されます。 |

### コレクタマネージャアプライアンス固有のポート

Sentinel コレクタマネージャアプライアンスでは、上記のポートに加えて次のポートが開いています。

| ポート | 説明 |
| --- | --- |
| TCP 22 | シェルが Sentinel アプライアンスに安全にアクセスできるようにするために使用されます。 |
| TCP 54984 | Sentinel アプライアンスの管理コンソール (WebYaST) で使用されます。Sentinel アプライアンスのアップデートサービスにも使用されます。 |
| TCP 289 | Audit の接続用に 1289 に転送されます。 |
| UDP 514 | Syslog メッセージ用に 1514 に転送されます。 |
| TCP 1290 | SuSE Firewall を介した接続が許可される Sentinel リンクポートです。 |
| UDP および TCP 40000 - 41000 | syslog などのデータ収集サーバの設定に使用可能なポートです。Sentinel は、これらのポートをデフォルトではリスンしません。 |

## 1.3.3 相関エンジン

### ネットワークポート

Sentinel 相関エンジンが正常に動作するよう、ファイアウォール上で次のポートが開かれていることを確認してください。

| ポート | 説明 |
| --- | --- |
| TCP 1099 および 2000 | 監視ツールが Java Management Extensions (JMX) を利用して Sentinel サーバプロセスに接続するのに使用されます。 |

### 相関エンジンアプライアンス固有のポート

Sentinel 相関エンジンアプライアンスでは、上記のポートに加えて次のポートが開いています。

| ポート | 説明 |
| --- | --- |
| TCP 22 | シェルが Sentinel アプライアンスに安全にアクセスできるようにするために使用されます。 |
| TCP 54984 | Sentinel アプライアンスの管理コンソール (WebYaST) で使用されます。Sentinel アプライアンスのアップデートサービスにも使用されます。 |

# 2 Sentinel のインストール

Sentinel は、スタンドアロンまたはアプライアンスとしてインストールできます。スタンドアロンインストーラは、既存の SUSE Linux Enterprise Server (SLES) 11 SP1 または Red Hat Enterprise Linux (RHEL) 6 オペレーティングシステム上に Sentinel をインストールします。アプライアンスインストーラは、SLES 11 SP1 64 ビットオペレーションシステムおよび Sentinel の両方をインストールします。

このセクションでは、既存の SLES 11 SP1 システムまたは RHEL 6 に Sentinel サーバをスタンドアロンでインストールする手順を説明します。アプライアンスインストールについては、41 ページの第 5 章「アプライアンスのインストール」を参照してください。



## 2.1 インストール方法

スタンドアロンインストールでは、次の方法を使用できます。

- **Interactive:** ユーザの入力によってインストールを進行します。インストール中にインストールオプション ( ユーザ入力またはデフォルト値 ) をファイルに記録でき、これを後でサイレントインストールに使用できます。
- **サイレント :** インストールオプションが事前に記録されている場合に、このオプションを使用できます。サイレントインストールではインストール時の入力内容を記録しているファイルを参照し、このファイル内に保存されている値を使用してインストールを実行します。使用する環境に同じ設定のレプリカを多数インストールする場合は、サイレントインストールが効果的です。詳細については、29 ページのセクション 2.5「サイレントインストール」を参照してください。

Sentinel のインタラクティブインストールとサイレントインストールのどちらも、root ユーザとしても非 root ユーザとしても実行できます。

### 2.1.1 標準およびカスタムインストール

Sentinel をインストールする場合、次の環境設定を使用できます。

- **Standard:** この環境設定では、インストールの環境設定のセットアップにデフォルト値を使用します。ユーザ入力は、パスワードについてのみ必要です。標準環境設定による Sentinel のインストールの詳細については、26 ページのセクション 2.4.1「標準環境設定」を参照してください。
- ［**Custom**］**:** この環境設定では、インストールの際に環境設定のセットアップでユーザに値を入力するよう求めます。ユーザはデフォルト値を選択するか、または必要な値を指定できます。カスタム環境設定による Sentinel のインストールの詳細については、27 ページのセクション 2.4.2「カスタム環境設定」を参照してください。

| 標準環境設定 | カスタム環境設定 |
|---|---|
| デフォルトの 90 日間の評価版キーを使用してインストールします。 | 90 日間有効のライセンスキーまたは有効なライセンスキーを使用してインストールできます。 |
| 管理者パスワードを指定し、その管理者パスワードを dbauser と appuser の両方に対するデフォルトパスワードとして使用できます。 | 管理者パスワードを指定できます。dbauser と appuser については、新しいパスワードを指定することも、管理者パスワードを使用することもできます。 |
| すべてのコンポーネントに対してデフォルトポートをインストールします。 | コンポーネント別にポートを指定できます。 |
| 内部データベースでユーザを認証します。 | 内部データベースでユーザを認証するか、または LDAP 認証を使用するかを選択できます。 |

### 2.1.2 インストールされるコンポーネント

Sentinel には複数のコンポーネントがあります。次のコンポーネントはすべてデフォルトでインストールされます。

- Sentinel サーバ
- 相関エンジン
- コレクタマネージャ

追加の相関エンジンまたはコレクタマネージャは、異なるシステム上にインストールできます。

## 2.2 開始準備

インストールを開始する前に、次の作業を完了していることを確認してください。

- ハードウェアおよびソフトウェアが、11 ページのセクション 1.1「システム要件とサポートされるプラットフォーム」に示されているシステム要件を満たしていることを確認します。
- 以前に Sentinel がインストールされていた環境の場合は、以前のインストール環境のファイルやシステム設定が残っていないことを確認します。詳細については、101 ページのパート V「アンインストール中」を参照してください。

- Sentinel サーバのパフォーマンス、安定性、信頼性を最適化するには、SLES では ext3 ファイルシステムを、RHEL では ext4 ファイルシステムを使用します。ファイルシステムの詳細については、『*ストレージ管理ガイド*』の「Linux ファイルシステムの概要 (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html)」を参照してください。
- ネットワーク設定は、システムに有効な IP アドレスと有効なホスト名が設定されるように構成します。
- ライセンスされたバージョンをインストールする場合は、ノベルカスタマケアセンター (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) からライセンスキーを取得します。
- Network Time Protocol (NTP) を使用して時刻を同期します。
- 19 ページのセクション 1.3「使用するポート」に示されているポートがファイアウォールで開かれていることを確認します。
- パフォーマンスを最適化するには、メモリ設定を PostgreSQL データベースに適した設定にします。

  SHMMAX パラメータは、1073741824 以上に設定する必要があります。適切な値を設定するには、次の情報を /etc/sysctl.conf ファイルに追加してください。

  ```
  # for Sentinel Postgresql
  kernel.shmmax=1073741824
  ```

- 最小構成インストールまたはヘッドレスインストールの場合は、Sentinel サーバのオペレーティングシステムに、少なくても SLES サーバまたは RHEL 6 サーバの Base Server コンポーネントを組み込む必要があります。Sentinel では、次の RPM の 64 ビットバージョンが必要です。
  - bash
  - bc
  - coreutils
  - glibc
  - grep
  - libgcc
  - libstdc
  - lsof
  - net-tools
  - openssl
  - python-libs
  - sed
  - zlib

## 2.3 インストールオプション

./install-sentinel --help は、次のオプションを示します。

| オプション | 値 | 説明 |
|---|---|---|
| --location | ディレクトリ | Sentinel をインストールする、root (/) 以外のディレクトリを指定します。 |
| -m、--manifest | ファイル名 | デフォルトのマニフェストファイルの代わりに使用する製品マニフェストファイルを指定します。 |
| --no-configure | | インストール後に製品を設定しないことを指定します。 |
| -n、--no-start | | インストールまたは設定後に Sentinel を起動または再起動しないことを指定します。 |
| -r、--recordunattended | ファイル名 | 無人インストールで使用するパラメータを記録するファイルを指定します。 |
| -u、--unattended | ファイル名 | 指定されたファイルにあるパラメータを使用して、無人のシステム上に Sentinel をインストールします。 |
| -h、--help | | Sentinel のインストール中に使用できるオプションを表示します。 |
| -l、--log-file | ファイル名 | ログメッセージをファイルに記録します。 |
| --no-banner | | バナーメッセージの表示を抑制します。 |
| -q、--quiet | | メッセージ数を減らします。 |
| -v、--verbose | | インストール時にすべてのメッセージを表示します。 |

## 2.4 インタラクティブインストール


- 26 ページのセクション 2.4.1「標準環境設定」
- 27 ページのセクション 2.4.2「カスタム環境設定」


### 2.4.1 標準環境設定

1 ノベル製品ダウンロード Web ページ (http://download.novell.com/index.jsp) から Sentinel インストールファイルをダウンロードします。

   **1a** ［*製品または技術*］フィールドで［*SIEM-Sentinel*］をブラウズして選択します。

   **1b** ［*検索*］をクリックします。

   **1c** ［*Sentinel 7.0 Evaluation*］の［*ダウンロード*］列のボタンをクリックします。

   **1d** ［*ダウンロードに進む*］をクリックし、お客様名とパスワードを入力します。

   **1e** お使いのプラットフォーム用のインストールバージョンに該当する［*ダウンロード*］をクリックします。

2 コマンドラインで次のコマンドを指定して、インストールファイルを抽出します。

```
tar zxvf <install_filename>
```

   *<install_filename>* は、実際のインストールファイル名に置き換えます。

3 インストーラを抽出したディレクトリに移動します。

```
cd sentinel_server-7.0.0.0.x86_64
```

4 次のコマンドを指定して、Sentinel をインストールします。

```
./install-sentinel
```

または

複数のシステムに Sentinel をインストールする場合は、インストールオプションをファイルに記録しておくことができます。このファイルを、他のシステムに対する Sentinel の無人インストールに使用できます。インストールオプションを記録するには、次のコマンドを指定します。

```
./install-sentinel -r <response_filename>
```

5 インストールに使用する言語の番号を指定してから、<Enter> を押します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

6 スペースキーを押して使用許諾契約を確認します。

7 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。

インストールパッケージをロードして環境設定のタイプの選択が求められるまで数秒かかることがあります。

8 選択を求められたら、「1」を指定して標準環境設定に進みます。

インストーラに付属の 90 日間の評価版ライセンスキーを使用してインストールを続行します。このライセンスキーは、90 日の評価期間中すべての製品機能を有効にします。評価期間中または評価期間終了後の任意の時点で、評価版のライセンスを購入したライセンスキーで置き換えることができます。

9 管理者ユーザ admin のパスワードを指定します。

10 パスワードを再度確認します。

このパスワードは、admin、dbauser、および appuser が使用します。

Sentinel のインストールが終了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

Sentinel Web インタフェースにアクセスするには、Web ブラウザに次の URL を入力します。

```
https://<IP_Address_Sentinel_server>:8443.
```

*<IP_Address_Sentinel_server>* は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

## 2.4.2 カスタム環境設定

カスタム環境設定で Sentinel をインストールする場合、ライセンスキーを指定したり、ユーザごとにパスワードを変更したり、内部コンポーネントとのやり取りに使用されるポートごとに値を指定したりすることができます。

1 ノベル製品ダウンロード Web ページ (http://download.novell.com/index.jsp) から Sentinel インストールファイルをダウンロードします。

**1a** ［*製品または技術*］フィールドで［*SIEM-Sentinel*］をブラウズして選択します。

**1b** ［*検索*］をクリックします。

**1c** ［*Sentinel 7.0 Evaluation*］の［*ダウンロード*］列のボタンをクリックします。

**1d** ［*ダウンロードに進む*］をクリックし、お客様名とパスワードを入力します。

**1e** お使いのプラットフォーム用のインストールバージョンに該当する［*ダウンロード*］をクリックします。

**2** コマンドラインで次のコマンドを指定して、インストールファイルを抽出します。

```
tar zxvf <install_filename>
```

<*install_filename*> は、実際のインストールファイル名に置き換えます。

**3** 抽出されたディレクトリのルートで次のコマンドを指定して、Sentinel をインストールします。

```
./install-sentinel
```

または

このカスタム環境設定を使用して複数のシステムに Sentinel をインストールする場合は、インストールオプションをファイルに記録しておくことができます。このファイルを、他のシステムに対する Sentinel の無人インストールに使用できます。インストールオプションを記録するには、次のコマンドを指定します。

```
./install-sentinel -r <response_filename>
```

**4** インストールに使用する言語の番号を指定してから、<Enter> を押します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

**5** スペースキーを押して使用許諾契約を確認します。

**6**「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。

インストールパッケージをロードして環境設定のタイプの選択が求められるまで数秒かかることがあります。

**7** Sentinel のカスタム環境設定を実行する場合は、「2」を指定します。

**8** デフォルトの 90 日間の評価版ライセンスキーを使用するには、「1」を入力します。

または

購入した Sentinel ライセンスキーを入力するには、「2」を入力します。

**9** 管理者ユーザ admin のパスワードを指定し、パスワードを再度確認します。

**10** データベースユーザ dbauser のパスワードを指定し、パスワードを再度確認します。

dbauser アカウントは、Sentinel がデータベースとのやり取りに使用する ID です。ここで入力するパスワードは、管理者パスワードを忘れた場合や紛失した場合の管理者パスワードのリセット操作を含む、データベース保守タスクの実行に使用します。

**11** アプリケーションユーザ appuser のパスワードを指定し、パスワードを再度確認します。

**12** 目的の番号を入力してから新しいポート番号を指定して、Sentinel サービスのポート割り当てを変更します。

**13** ポートを変更してから「7」を指定し、完了します。

**14** 内部データベースのみを使用してユーザを認証するには、「1」を入力します。

または

ドメインで LDAP ディレクトリを設定している場合に、LDAP ディレクトリ認証を使用してユーザを認証するには、「2」を入力します。

デフォルト値は 1 です。

Sentinel のインストールが終了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

Sentinel Web インタフェースにアクセスするには、Web ブラウザに次の URL を入力します。

```
https://<IP_Address_Sentinel_server>:8443.
```

*<IP_Address_Sentinel_server>* は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

## 2.5 サイレントインストール

複数の Sentinel サーバをインストールして展開する必要がある場合は、Sentinel サーバのサイレントインストール ( 無人インストール ) が便利です。そのような場合には、インタラクティブインストール時にインストールパラメータを記録し、記録したファイルをその他すべてのサーバで実行します。標準環境設定またはカスタム環境設定による Sentinel のインストール中に、インストールパラメータを記録できます。

サイレントインストールを実行する場合、インストールパラメータをファイルに記録してあることを確認してください。レスポンスファイルの作成については、26 ページのセクション 2.4.1「標準環境設定」または27 ページのセクション 2.4.2「カスタム環境設定」を参照してください。

1. ノベル製品ダウンロード Web ページ (http://download.novell.com/index.jsp) からインストールファイルをダウンロードします。
2. Sentinel をインストールするサーバに roo t としてログインします。
3. 次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

   ```
   tar -zxvf <install_filename>
   ```

   *<install_filename>* は、実際のインストールファイル名に置き換えます。
4. 次のコマンドを指定して、Sentinel をサイレントモードでインストールします。

   ```
   ./install-sentinel -u <response_file>
   ```

   インストールは、レスポンスファイルに格納された値を使用して進行します。

   Sentinel のインストールが終了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

Sentinel Web インタフェースにアクセスするには、Web ブラウザに次の URL を入力します。

```
https://<IP_Address_Sentinel_server>:8443.
```

*<IP_Address_Sentinel_server>* は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

## 2.6 非 root ユーザとして Sentinel をインストール

組織のポリシーによって、root として Sentinel の完全なインストールを実行することができない場合は、他のユーザとして Sentinel をインストールできます。このインストール手順では、いくつかの手順は root ユーザとして実行し、その後、root ユーザが作成した他のユーザとして Sentinel のインストールを続行します。最後に、root ユーザでインストールを完了します。

1. ノベル製品ダウンロード Web ページ (http://download.novell.com/index.jsp) からインストールファイルをダウンロードします。
2. コマンドラインで次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

   ```
   tar -zxvf <install_filename>
   ```

   <*install_filename*> は、実際のインストールファイル名に置き換えます。
3. root として Sentinel をインストールするサーバに root としてログインします。
4. 次のコマンドを指定します。

   ```
   ./bin/root_install_prepare
   ```

   root 権限で実行するコマンドの一覧が表示されます。非 root ユーザにデフォルト以外の場所に Sentinel をインストールさせたい場合は、コマンドに加えて --location オプションも指定します。例 :

   ```
   ./bin/root_install_prepare --location=/foo
   ```

   --location オプションに渡す値 foo は、ディレクトリパスの前に付加されます。

   これによって、novell グループおよび novell ユーザが存在しなければ、それらが作成されます。
5. コマンドリストを受け入れます。

   表示されたコマンドが実行されます。
6. 次のコマンドを指定して、新しく作成された、root でない novell ユーザに変更します : novell:

   su novell
7. ( 条件による ) インタラクティブインストールを実行するには :

   **7a** 次のコマンドを指定します。

   ```
   ./install-sentinel
   ```

   デフォルト以外の場所に Sentinel をインストールするには、コマンドに加えて --location オプションを指定します。例 :.

   ```
   ./install-sentinel --location=/foo
   ```

   **7b** ステップ 9 に進みます。
8. ( 条件による ) サイレントインストールを実行するには :

   **8a** 次のコマンドを指定します。

   ```
   ./install-sentinel -u <response_file>
   ```

   インストールは、レスポンスファイルに格納された値を使用して進行します。

   **8b** ステップ 12 に進みます。
9. インストールに使用する言語の番号を指定します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

10 エンドユーザの使用許諾契約を読み、「yes」または「y」と入力して契約に同意し、インストールを続行します。

すべての RPM パッケージのインストールが開始されます。このインストールが完了するまで数秒かかることがあります。

11 インストールのモードを指定するように求められます。

- 標準環境設定で続行する場合は、26 ページのセクション 2.4.1「標準環境設定」のステップ 8 からステップ 10 に従って手順を進めます。
- カスタム環境設定で続行する場合は、27 ページのセクション 2.4.2「カスタム環境設定」のステップ 7 からステップ 14 に従って手順を進めます。

12 root ユーザとしてログインし、次のコマンドを指定してインストールを完了します。

```
./bin/root_install_finish
```

Sentinel のインストールが終了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

Sentinel Web インタフェースにアクセスするには、Web ブラウザに次の URL を入力します。

```
https://<IP_Address_Sentinel_server>:8443.
```

*<IP_Address_Sentinel_server>* は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

## 2.7 インストール後の環境設定の変更

Sentinel のインストール後に、有効なライセンスキーを入力したり、パスワードを変更したり、割り当てられたポートを変更したりする場合は、configure.sh スクリプトを実行してこれらの変更を行います。スクリプトは /opt/novell/sentinel/setup フォルダにあります。

1 コマンドラインで次のコマンドを指定して、configure.sh スクリプトを実行します。

```
./configure.sh
```

2 Sentinel の標準環境設定を実行するには、「1」を指定します。カスタム環境設定を実行する場合は、「2」を指定します。

3 スペースキーを押して使用許諾契約を確認します。

4 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。

インストールパッケージをロードするのに数秒かかることがあります。

5 デフォルトの 90 日間の評価版ライセンスキーを使用するには、「1」を入力します。

または

購入した Sentinel ライセンスキーを入力するには、「2」を入力します。

6 管理者ユーザ admin の既存のパスワードをそのまま使用するかどうか決定します。

- 既存のパスワードをそのまま使用するには、「1」を入力してからステップ 7 に進みます。
- 既存のパスワードを変更するには「2」を入力し、新しいパスワードを指定して確認してから、ステップ 7 に進みます。

7 データベースユーザ dbauser の既存のパスワードをそのまま使用するかどうか決定します。

- 既存のパスワードをそのまま使用するには、「1」を入力してからステップ 8 に進みます。
- 既存のパスワードを変更するには「2」を入力し、新しいパスワードを指定して確認してから、ステップ 8 に進みます。

dbauser アカウントは、Sentinel がデータベースとのやり取りに使用する ID です。ここで入力するパスワードは、管理者パスワードを忘れた場合や紛失した場合の管理者パスワードのリセット操作を含む、データベース保守タスクの実行に使用します。

8 アプリケーションユーザ appuser の既存のパスワードをそのまま使用するかどうか決定します。

- 既存のパスワードをそのまま使用するには、「1」を入力してからステップ 9 に進みます。
- 既存のパスワードを変更するには「2」を入力し、新しいパスワードを指定して確認してから、ステップ 9 に進みます。

dbauser アカウントは、Sentinel がデータベースとのやり取りに使用する ID です。ここで入力するパスワードは、管理者パスワードを忘れた場合や紛失した場合の管理者パスワードのリセット操作を含む、データベース保守タスクの実行に使用します。

9 目的の番号を入力してから新しいポート番号を指定して、Sentinel サービスのポート割り当てを変更します。

10 ポートを変更してから「7」を指定し、完了します。

11 内部データベースのみを使用してユーザを認証するには、「1」を入力します。

または

ドメインで LDAP ディレクトリを設定している場合に、LDAP ディレクトリ認証を使用してユーザを認証するには、「2」を入力します。

デフォルト値は 1 です。

# 3 追加のコレクタマネージャのインストール

Sentinel では、デフォルトで単一のコレクタマネージャがインストールされます。環境によっては、複数のコレクタマネージャが必要な場合があります。リモートのコレクタマネージャをインストールするには、次の情報を使用します。

**IMPORTANT**: Sentinel を実行している同じサーバ上には、コレクタマネージャまたは相関エンジンを追加でインストールすることはできません。



## 3.1 追加のコレクタマネージャの利点

分散ネットワーク環境で複数のコレクタマネージャをインストールすると、次のような利点があります。

- **システムのパフォーマンスの向上 :** コレクタマネージャを追加すると、分散環境でイベントデータを解析および処理できるため、システムのパフォーマンスが向上します。
- **データのセキュリティの強化およびネットワーク帯域幅要件の低下 :** コレクタマネージャがイベントソースと同じ場所にあると、フィルタ、暗号化、およびデータの圧縮を同じソースで実行できます。
- **ファイルキャッシング :** サーバでイベントのアーカイブなどの処理が一時的に大量に発生した場合、リモートのコレクタマネージャは大量のデータをキャッシュできます。この機能は、イベントキャッシングをネイティブでサポートしない Syslog などのプロトコルの場合に役立ちます。

## 3.2 開始準備

インストールを開始する前に、次の作業を完了していることを確認してください。

❒ ハードウェアとソフトウェアが最低要件を満たしていることを確認します。詳細については、11 ページのセクション 1.1「システム要件とサポートされるプラットフォーム」を参照してください。

- Network Time Protocol (NTP) を使用して時刻を同期します。
- コレクタマネージャは、Sentinel サーバ上のメッセージバスポート (61616) にネットワーク接続する必要があります。コレクタマネージャのインストールを開始する前に、すべてのファイアウォールおよびネットワーク設定で、このポートでの通信が許可されていることを確認します。

## 3.3 追加のコレクタマネージャのインストール

リモートのコレクタマネージャは、Sentinel またはリモートの相関エンジンがインストールされているのとは異なるシステムにインストールする必要があります。

1. Web ブラウザに次の URL を入力して、Sentinel Web インタフェースを起動します。

   `https://<IP_Address_Sentinel_server>:8443.`

   <*IP_Address_Sentinel_server*> は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

   Sentinel サーバのインストール時に指定したユーザ名およびパスワードでログインします。
2. ツールバーで［*ダウンロード*］をクリックします。
3. ［コレクタマネージャ］の下の［*インストーラのダウンロード*］をクリックします。
4. ［*ファイルの保存*］をクリックして、目的の場所にインストーラを保存します。
5. 次のコマンドを指定して、インストールファイルを抽出します。

   `tar zxvf <install_filename>`

   <*install_filename*> は、実際のインストールファイル名に置き換えます。
6. インストーラを抽出したディレクトリに移動します。例 :

   `cd sentinel_collector_mgr-7.0.0.0.x86_64`
7. 次のコマンドを指定して、Sentinel コレクタマネージャをインストールします。

   `./install-cm`

   インストールスクリプトは、使用可能なメモリとディスク領域を最初にチェックします。使用可能なメモリが 1.5GB よりも少ない場合、スクリプトは自動的にインストールを終了します。
8. インストールに使用する言語の番号を指定します。

   エンドユーザの使用許諾契約が、選択した言語で表示されます。
9. スペースキーを押して使用許諾契約を確認します。
10. 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。

    環境設定のタイプの選択が求められるまで数秒かかることがあります。
11. 選択を求められたら、「1」を指定して標準環境設定に進みます。
12. デフォルトの Communication Server ホスト名または、Sentinel がインストールされているマシンの IP アドレスを入力します。
13. コレクタマネージャのユーザ名とパスワードを指定します。

    ユーザ名とパスワードは、Sentinel サーバにある /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。

例 :

```
collectormanager=1c51ae55
```

この例では、collectormanager はユーザ名であり、対応する値はパスワードです。

14 証明書に同意するよう求められたら常に同意します。

リモートの Sentinel コレクタマネージャのインストールが完了しました。

## 3.4 コレクタマネージャのカスタムユーザの追加

Sentinel では、デフォルトのコレクタマネージャユーザ名 collectormanager の使用が推奨されます。ただし、リモートのコレクタマネージャを複数インストールしており、それぞれを個別に識別する必要がある場合は、新しいユーザを作成できます。

1 Sentinel のインストールファイルにアクセスできるユーザとしてサーバにログインします。

2 activemqgroups.properties ファイルを開きます。

このファイルは /<*install_dir*>/etc/opt/novell/sentinel/config/ ディレクトリにあります。

3 コレクタマネージャの新しいユーザを、カンマで区切って cm セクションに追加します。例 :

```
cm=collectormanager,cmuser1,cmuser2,...
```

4 ファイルを保存して閉じます。

5 activemqusers.properties ファイルを開きます。

このファイルは /<*install_dir*>/etc/opt/novell/sentinel/config/ ディレクトリにあります。

6 ステップ 3 で作成したユーザのパスワードを追加します。

このパスワードには任意のランダムな文字列を指定できます。例 :

```
system=c7f34372ecd20d831cceb29e754e5ac9
collectormanager=1c51ae56
cmuser1=1b51de55
cmuser2=1a51ce57
```

7 ファイルを保存して閉じます。

8 Sentinel サーバを再起動します。

# 4 追加の相関エンジンのインストール

デフォルトでは、Sentinel は単一の相関エンジンをインストールします。多くの相関ルールがある、またはイベントレートが非常に高い環境では、複数の相関エンジンをインストールすると便利です。相関エンジンあたりの推奨されるイベントレートについては、11 ページの第 1 章「システム要件を満たす」の相関エンジンを参照してください。

---

**IMPORTANT**: Sentinel を実行しているサーバ上には、コレクタマネージャまたは相関エンジンを追加でインストールすることはできません。

---



## 4.1 開始準備

インストールを開始する前に、次の作業を完了していることを確認してください。

- ❒ ハードウェアとソフトウェアが最低要件を満たしていることを確認します。詳細については、11 ページのセクション 1.1「システム要件とサポートされるプラットフォーム」を参照してください。
- ❒ Network Time Protocol (NTP) を使用して時刻を同期します。
- ❒ 相関エンジンは、Sentinel サーバ上のメッセージバスポート (61616) にネットワーク接続する必要があります。相関エンジンのインストールを開始する前に、すべてのファイアウォールおよびネットワーク設定で、このポートでの通信が許可されていることを確認します。

## 4.2 追加の相関エンジンのインストール

リモートの相関エンジンは、Sentinel またはリモートのコレクタマネージャがインストールされているのとは異なるシステムにインストールする必要があります。

1. Web ブラウザに次の URL を入力して、Sentinel Web インタフェースを起動します。

   `https://<IP_Address_Sentinel_server>:8443.`

   *<IP_Address_Sentinel_server>* は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

   Sentinel サーバのインストール時に指定したユーザ名およびパスワードでログインします。
2. ツールバーで［*ダウンロード*］をクリックします。
3. ［相関エンジン］の下の［*インストーラのダウンロード*］をクリックします。

4 ［*ファイルの保存*］をクリックして、目的の場所にインストーラを保存します。

5 次のコマンドを指定して、インストールファイルを抽出します。

```
tar zxvf <install_filename>
```

<*install_filename*> は、実際のインストールファイル名に置き換えます。

6 インストーラを抽出したディレクトリに移動します。例 :

```
cd sentinel_correlation_engine-7.0.0.0.x86_64
```

7 次のコマンドを指定して、Sentinel 相関エンジンをインストールします。

```
./install-ce
```

インストールスクリプトは、使用可能なメモリとディスク領域を最初にチェックします。使用可能なメモリが 1.5GB よりも少ない場合、スクリプトは自動的にインストールを終了します。

8 インストールに使用する言語の番号を指定します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

9 スペースキーを押して使用許諾契約を確認します。

10 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。

インストールパッケージをロードして環境設定のタイプの選択が求められるまで数秒かかることがあります。

11 選択を求められたら、「1」を指定して標準環境設定に進みます。

12 デフォルトの Communication Server ホスト名または、Sentinel がインストールされているマシンの IP アドレスを入力します。

13 相関エンジンのユーザ名とパスワードを指定します。

ユーザ名とパスワードは、Sentinel サーバにある /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。

例 :

```
correlationengine=68790d7a
```

この例では、correlationengine はユーザ名であり、対応する値はパスワードです。

14 証明書に同意するよう求められたら常に同意します。

リモートの Sentinel 相関エンジンのインストールが完了しました。

## 4.3 相関エンジンのカスタムユーザの追加

Sentinel では、デフォルトの相関エンジンユーザ名 correlationengine の使用が推奨されます。ただし、リモートの相関エンジンを複数インストールしており、それぞれを個別に識別する必要がある場合は、新しいユーザを作成できます。

1 Sentinel のインストールファイルにアクセスできるユーザとしてサーバにログインします。

2 activemqgroups.properties ファイルを開きます。

このファイルは /<*install_dir*>/etc/opt/novell/sentinel/config/ ディレクトリにあります。

3 相関エンジンの新しいユーザを、カンマで区切って admin セクションに追加します。例 :

```
admins=system,correlationengine,ceuser1,ceuser2,...
```

4 ファイルを保存して閉じます。

5 activemqusers.properties ファイルを開きます。

このファイルは /<*install_dir*>/etc/opt/novell/sentinel/config/ ディレクトリにあります。

6 ステップ 3 で作成したユーザのパスワードを追加します。

このパスワードには任意のランダムな文字列を指定できます。例 :

```
system=c7f34372ecd20d831cceb29e754e5ac9
correlationengine=68790d7a
ceuser1=69700c6d
ceuser2=70701b5c
```

7 ファイルを保存して閉じます。

8 Sentinel サーバを再起動します。

# 5 アプライアンスのインストール

Sentinel アプライアンスは SUSE Studio で構築された、すぐに実行可能なソフトウェアアプライアンスです。このアプライアンスは、強化された SUSE Linux Enterprise Server (SLES) 11 SP 1 オペレーティングシステムと、Sentinel ソフトウェアの統合されたアップデートサービスを組み合わせて、お客様が既存の投資を活用できるよう、簡単でシームレスなユーザエクスペリエンスを提供します。ソフトウェアアプライアンスは、ハードウェアまたは仮想環境にインストールできます。



## 5.1 開始準備

アプライアンスのインストールを開始する前に、次の作業を完了していることを確認してください。

- ❒ ハードウェア要件が満たされていることを確認します。詳細については、11 ページのセクション 1.1「システム要件とサポートされるプラットフォーム」を参照してください。
- ❒ ライセンスされたバージョンをインストールする場合は、ノベルカスタマケアセンター (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) からライセンスキーを取得します。
- ❒ ノベルカスタマケアセンター (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) から登録コードを取得して、ソフトウェアのアップデートを登録します。

## 5.2 VMware アプライアンスのインストール

### 5.2.1 Sentinel のインストール

VMware ESX サーバに Sentinel アプライアンスイメージをインポートしてインストールするには :

1. ノベル製品ダウンロードのサイト (http://download.novell.com/index.jsp) から VMware アプライアンスのインストールファイルをダウンロードします。

   VMware アプライアンスの正しいファイル名には vmx が含まれますたとえば、sentinel_server_7.0.0.0.x86_64.vmx.tar.gz などです。

2. アプライアンスイメージのインストール先となる ESX データストアを確立します。
3. アプライアンスをインストールするサーバに Administrator としてログインします。
4. 次のコマンドを指定して、VM Converter がインストールされているマシンから圧縮されたアプライアンスイメージを抽出します。

   ```
   tar zxvf <install_file>
   ```

   <*install_filename*> は、実際のファイル名に置き換えます。

5. VMware イメージを ESX サーバにインポートするには、VMware Converter を使用して、インストールウィザードの画面の指示に従います。
6. ESX サーバマシンにログインします。
7. インポートしたアプライアンスの VMware イメージを選択して、［*電源オン*］アイコンをクリックします。
8. 使用する言語を選択して、［*次へ*］をクリックします。
9. キーボードのレイアウトを選択して、［*次へ*］をクリックします。
10. SUSE Linux Enterprise Server (SLES) 11 SP1 ソフトウェア使用許諾契約書の条項を確認して同意します。
11. NetIQ Sentinel の使用許諾契約の条項を確認して同意します。
12. ［ホスト名］および［ドメイン名］ページで、ホスト名とドメイン名を指定してから、［*ホスト名をループバック IP に割り当てる*］オプションが選択されていることを確認します。
13. ［*次へ*］をクリックします。ホスト名の環境設定が保存されます。
14. 次のいずれかの操作を行います。
    - 現在のネットワーク接続設定を使用するには、［ネットワーク環境設定 II］ページで［*次の環境設定を使用する*］を選択して、［*次へ*］をクリックます。
    - ネットワーク接続設定を変更するには、［*変更*］を選択して目的の変更を行ってから、［*次へ*］をクリックします。

    ネットワーク接続設定が保存されます。

15. 日付と時刻を設定して、［*次へ*］をクリックします。

    インストール後に NTP 環境設定を変更するには、アプライアンスのコマンドラインから YaST を使用します。WebYast を使用して日付と時刻を変更することはできますが、NTP の環境設定を変更することはできません。

    インストール直後に時刻が同期されていない場合は、次のコマンドを実行して NTP を再起動します。

    ```
    rcntp restart
    ```

16. root のパスワードを設定して、［*次へ*］をクリックします。

使用可能なメモリとディスク領域がチェックされます。使用可能なメモリが 2.5GB よりも少ない場合、インストールは続行できません。［*次へ*］ボタンはグレー表示となり、使用できません。

使用可能なメモリが 2.5GB 以上 6.7GB 未満の場合、推奨よりもメモリの容量が少ないというメッセージが表示されます。このメッセージが表示されたら、［*次へ*］をクリックしてインストールを続行します。

**17** Sentinel 管理者のパスワードを設定してから、［*次へ*］をクリックします。

システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

**18** コンソールに表示されたアプライアンスの IP アドレスをメモします。

**19** 52 ページのセクション 5.5「アプライアンスのインストール後の環境設定」に従って手順を進めます。

## 5.2.2 コレクタマネージャのインストール

VMware ESX サーバにアプライアンスイメージをインポートしてインストールするには :

**1** ノベル製品ダウンロードのサイト (http://download.novell.com/index.jsp) から VMware アプライアンスのインストールファイルをダウンロードします。

VMware アプライアンスの正しいファイル名には vmx が含まれますたとえば、sentinel_colletor_manager_7.0.0.0.x86_64.vmx.tar.gz などです。

**2** アプライアンスイメージのインストール先となる ESX データストアを確立します。

**3** アプライアンスをインストールするサーバに Administrator としてログインします。

**4** 次のコマンドを指定して、VM Converter がインストールされているマシンから圧縮されたアプライアンスイメージを抽出します。

```
tar zxvf <install_file>
```

<*install_filename*> は、実際のファイル名に置き換えます。

**5** VMware イメージを ESX サーバにインポートするには、VMware Converter を使用して、インストールウィザードの画面の指示に従います。

**6** ESX サーバマシンにログインします。

**7** インポートしたアプライアンスの VMware イメージを選択して、［*電源オン*］アイコンをクリックします。

**8** コレクタマネージャが接続する Sentinel サーバのホスト名または IP アドレスを指定します。

**9** Communication Server のポート番号を指定します。デフォルトのメッセージバスのポートは 61616 です。

**10** JMS ユーザ名を指定します。これは、コレクタマネージャのユーザ名です。デフォルトのユーザ名は collectormanager です。

**11** JMS ユーザのパスワードを指定します。

ユーザ名とパスワードは、Sentinel サーバにある /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。

**12** ( オプション ) パスワードを確認するには、activemqusers.properties 内の次の行を確認します。

```
collectormanager=<password>
```

この例では、collectormanager はユーザ名であり、対応する値はパスワードです。

13 *[次へ]* をクリックします。

14 同意を求められたら、証明書に同意します。

15 [ *次へ* ] をクリックしてインストールを完了します。

インストールが完了したら、このアプライアンスが Sentinel コレクタマネージャであることと、IP アドレスを示すメッセージが表示されます。また、Sentinel サーバのユーザインタフェース IP アドレスも表示します。

### 5.2.3 相関エンジンのインストール

相関エンジンのインストールは、コレクタマネージャアプライアンスのインストールと似ています。

1 ノベル製品ダウンロードのサイト (http://download.novell.com/index.jsp) から VMware アプライアンスのインストールファイルをダウンロードします。

VMware 相関エンジンアプライアンスの正しいファイル名には vmx が含まれます。たとえば、sentinel_correlation_engine_7.0.0.0.x86_64.vmx.tar.gz などです。

2 アプライアンスイメージのインストール先となる ESX データストアを確立します。

3 アプライアンスをインストールするサーバに Administrator としてログインします。

4 次のコマンドを指定して、VM Converter がインストールされているマシンから圧縮されたアプライアンスイメージを抽出します。

```
tar zxvf <install_file>
```

<*install_filename*> は、実際のファイル名に置き換えます。

5 VMware イメージを ESX サーバにインポートするには、VMware Converter を使用して、インストールウィザードの画面の指示に従います。

6 ESX サーバマシンにログインします。

7 インポートしたアプライアンスの VMware イメージを選択して、［*電源オン*］アイコンをクリックします。

8 相関エンジンが接続する Sentinel サーバのホスト名または IP アドレスを指定します。

9 Communication Server のポート番号を指定します。デフォルトのメッセージバスのポートは 61616 です。

10 JMS ユーザ名を指定します。これは、相関エンジンのユーザ名です。デフォルトのユーザ名は correlationengine です。

11 JMS ユーザのパスワードを指定します。

ユーザ名とパスワードは、Sentinel サーバにある /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。

12 ( オプション ) パスワードを確認するには、activemqusers.properties ファイル内の次の行を確認します。

```
correlationengine=<password>
```

この例では、correlationengine はユーザ名であり、対応する値はパスワードです。

13 *[次へ]* をクリックします。

14 同意を求められたら、証明書に同意します。

15 [ *次へ* ] をクリックしてインストールを完了します。

インストールが終了したら、このアプライアンスが Sentinel 相関エンジンであることと、IP アドレスを示すメッセージが表示されます。また、Sentinel サーバのユーザインタフェース IP アドレスも表示します。

## 5.3 Xen アプライアンスのインストール


- 45 ページのセクション 5.3.1「Sentinel のインストール」
- 47 ページのセクション 5.3.2「コレクタマネージャのインストール」
- 48 ページのセクション 5.3.3「相関エンジンのインストール」


### 5.3.1 Sentinel のインストール

1 Xen 仮想アプライアンスのインストールファイルをノベル製品ダウンロードのサイト (http://download.novell.com/index.jsp) から /var/lib/xen/images にダウンロードします。

Xen 仮想アプライアンスの正しいファイル名には、xen が含まれますたとえば、Sentinel_7.0.0.0.x86_64.xen.tar.gz などです。

2 次のコマンドを指定して、ファイルをアンパックします。

```
tar -zxvf <install_file>
```

<*install_file*> は、実際のインストールファイル名に置き換えます。

3 新しいインストールディレクトリに移動します。このディレクトリには、次のファイルがあります。

- <*file_name*>.raw
- <*file_name*>.xenconfig

4 テキストエディタを使用して <*file_name*>.xenconfig ファイルを開きます。

5 このファイルを次のように変更します。

- disk 設定の .raw ファイルのフルパスを指定します。
- ネットワーク環境設定のブリッジ設定を指定します ( 例 : "bridge=br0" または "bridge=xenbr0")。
- name および memory の設定値を指定します。

例 :

```
# -*- mode: python; -*-
name="Sentinel_7.0.0.0.x86_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/sentinel_7.0.0.0.x86_64/
sentinel_7.0.0.0.x86_64.raw,xvda,w" ]
vif=[ "bridge=br0" ]
```

6 <*filename*>.xenconfig ファイルを修正したら、次のコマンドを指定して VM を作成します。

```
xm create <file_name>.xenconfig
```

7 ( オプション )VM が作成されたかどうかを確認するには、次のコマンドを指定します。

xm list

生成されるリストに VM が表示されます。

たとえば、.xenconfig ファイルに name="Sentinel_7.0.0.0.x86_64" と環境設定した場合、その名前に VM が付されます。

8 インストールを実行するには、次のコマンドを指定します。

```
xm console <vm name>
```

*<vm_name>* は、.xenconfig ファイルでの名前設定で指定された名前に置き換えます。これは、手順 7 で返された名前でもあります。例 :

xm console Sentinel_7.0.0.0.x86_64

最初に使用可能なメモリとディスク領域がチェックされます。使用可能なメモリが 2.5GB よりも少ない場合、インストールは自動的に終了します。使用可能なメモリが 2.5GB 以上 6.7GB 未満の場合、推奨よりもメモリの容量が少ないというメッセージが表示されます。インストールを続行する場合は「y」と入力し、続行しない場合は「n」と入力します。

9 使用する言語を選択して、［*次へ*］をクリックします。

10 キーボードのレイアウトを選択して、［*次へ*］をクリックします。

11 SUSE Linux Enterprise Server (SLES) 11 SP1 ソフトウェア使用許諾契約書の条項を確認して同意します。

12 NetIQ Sentinel の使用許諾契約の条項を確認して同意します。

13 ［ホスト名］および［ドメイン名］ページで、ホスト名とドメイン名を指定してから、［*ホスト名をループバック IP に割り当てる*］オプションが選択されていることを確認します。

14 ［*次へ*］を選択します。ホスト名の環境設定が保存されます。

15 次のいずれかの操作を行います。

- 現在のネットワーク接続設定を使用するには、［*ネットワーク環境設定 II*］ページで［*次の環境設定を使用する*］を選択します。
- ネットワーク接続設定を変更するには、［*変更*］を選択し、目的の変更を行います。

16 ［*次へ*］を選択します。ネットワーク接続設定が保存されます。

17 日付と時刻を設定して、［*次へ*］をクリックし、［*終了*］をクリックします。

インストール後に NTP 環境設定を変更するには、アプライアンスのコマンドラインから YaST を使用します。WebYast を使用して日付と時刻を変更することはできますが、NTP の環境設定を変更することはできません。

インストール直後に時刻が同期されていない場合は、次のコマンドを実行して NTP を再起動します。

```
rcntp restart
```

18 SUSE Enterprise Server の root のパスワードを設定して、［*次へ*］をクリックします。

19 Sentinel 管理者のパスワードを設定してから、［*次へ*］をクリックします。

Sentinel のインストールが続行されて完了します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

コンソールに表示されたアプライアンスの IP アドレスをメモします。

20 52 ページのセクション 5.5「アプライアンスのインストール後の環境設定」に従って手順を進めます。

### 5.3.2 コレクタマネージャのインストール

コレクタマネージャは、その最小ハードウェア要件を満足し、Xen が有効になっている Linux システム上に、アプライアンスとしてインストールすることができます。詳細については、12 ページのセクション 1.1.2「ハードウェア要件」を参照してください。

1. 45 ページのセクション 5.3.1「Sentinel のインストール」のステップ 1 からステップ 14 を実行します。

   Xen コレクタマネージャの仮想アプライアンスインストールファイルの正しいファイル名は、sentinel_collector_manager_7.0.0.0.x86_64.xen.tar.gz です。

2. ［ネットワーク環境設定 II］画面で［*変更*］を選択して、追加のコレクタマネージャアプライアンスをインストールする仮想マシンの IP アドレスを指定します。

3. 指定した IP アドレスのサブネットマスクを指定します。

4. ［*次へ*］を選択します。ネットワーク接続設定が保存されます。

5. 日付と時刻を設定して、［*次へ*］を選択します。

   インストール後に NTP 環境設定を変更するには、アプライアンスのコマンドラインから YaST を使用します。WebYast を使用して日付と時刻を変更することはできますが、NTP の環境設定を変更することはできません。

   インストール直後に時刻が同期されていない場合は、次のコマンドを実行して NTP を再起動します。

   ```
   rcntp restart
   ```

6. SUSE Enterprise Server の root のパスワードを設定して、［*次へ*］を選択します。

7. 相関エンジンが接続する Sentinel サーバのホスト名または IP アドレスを指定します。

8. Communication Server のポート番号を指定します。デフォルトのメッセージバスのポートは 61616 です。

9. JMS ユーザ名を指定します。これは、コレクタマネージャのユーザ名です。デフォルトのユーザ名は collectormanager です。

10. JMS ユーザのパスワードを指定します。

    ユーザ名とパスワードは、Sentinel サーバにある /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。

11. ( オプション ) パスワードを確認するには、activemqusers.properties ファイル内の次の行を確認します。

    ```
    collectormanager=<password>
    ```

    この例では、collectormanager はユーザ名であり、対応する値はパスワードです。

12. [ *次へ* ] を選択してインストールを完了します。

    インストールが完了したら、このアプライアンスが Sentinel コレクタマネージャであることと、IP アドレスを示すメッセージが表示されます。

### 5.3.3 相関エンジンのインストール

相関エンジンは、その最小ハードウェア要件を満足し、Xen が有効になっている Linux システム上に、アプライアンスとしてインストールすることができます。詳細については、12 ページのセクション 1.1.2「ハードウェア要件」を参照してください。

1. 45 ページのセクション 5.3.1「Sentinel のインストール」のステップ 1 からステップ 14 を実行します。

   Xen 相関エンジンの仮想アプライアンスインストールファイルの正しいファイル名は、sentinel_correlation_engine_7.0.0.0.x86_64.xen.tar.gz です。

2. [ ネットワーク環境設定 II] 画面で [ *変更* ] を選択して、相関エンジンアプライアンスをインストールする仮想マシンの IP アドレスを指定します。

3. 指定した IP アドレスのサブネットマスクを指定します。

4. *[次へ]* を選択します。ネットワーク接続設定が保存されます。

5. 日付と時刻を設定して、[*次へ*] を選択します。

   インストール後に NTP 環境設定を変更するには、アプライアンスのコマンドラインから YaST を使用します。WebYast を使用して日付と時刻を変更することはできますが、NTP の環境設定を変更することはできません。

   インストール直後に時刻が同期されていない場合は、次のコマンドを実行して NTP を再起動します。

   ```
   rcntp restart
   ```

6. SUSE Enterprise Server の root のパスワードを設定して、[*次へ*] を選択します。

7. 相関エンジンが接続する Sentinel サーバのホスト名または IP アドレスを指定します。

8. Communication Server のポート番号を指定します。デフォルトのメッセージバスのポートは 61616 です。

9. JMS ユーザ名を指定します。これは、相関エンジンのユーザ名です。デフォルトのユーザ名は correlationengine です。

10. JMS ユーザのパスワードを指定します。

11. *[次へ]* をクリックします。

    ユーザ名とパスワードは、Sentinel サーバにある /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。

12. パスワードを確認するには、activemqusers.properties ファイル内の次の行を確認します。

    ```
    correlationengine=<password>
    ```

    この例では、correlationengine はユーザ名であり、対応する値はパスワードです。

13. 同意を求められたら、証明書に同意します。

14. [ *次へ* ] をクリックしてインストールを完了します。

    インストールが完了したら、このアプライアンスが Sentinel 相関エンジンであることと、IP アドレスを示すメッセージが表示されます。また、Sentinel サーバのユーザインタフェース IP アドレスも表示します。

## 5.4 ハードウェアへのアプライアンスのインストール

ハードウェアにアプライアンスをインストールする前に、アプライアンス ISO ディスクイメージがサポートサイトからダウンロードされ、アンパックされて、DVD で使用可能になっていることを確認します。

---

**IMPORTANT**: ISO ディスクイメージを使用したハードウェア ( ベアメタルおよび Hyper-V) へのインストールを完了するには、最低 4.5GB のメモリが必要です。ハードウェア要件の詳細については、12 ページのセクション 1.1.2「ハードウェア要件」を参照してください。

---



### 5.4.1 Sentinel のインストール

1. DVD ドライブからその DVD を使用して物理マシンをブートします。
2. インストールウィザードの画面の指示に従います。
3. ブートメニューの一番上のエントリを選択して、ライブ DVD のアプライアンスイメージを実行します。

   最初に使用可能なメモリとディスク領域がチェックされます。使用可能なメモリが 2.5GB よりも少ない場合、インストールは自動的に終了します。使用可能なメモリが 2.5GB 以上 6.7GB 未満の場合、推奨よりもメモリの容量が少ないというメッセージが表示されます。インストールを続行する場合は「y」と入力し、続行しない場合は「n」と入力します。
4. 使用する言語を選択して、［*次へ*］をクリックします。
5. キーボードのレイアウトを選択して、［*次へ*］をクリックします。
6. SUSE Enterprise Server ソフトウェア使用許諾契約書の条項を確認して同意します。
7. NetIQ Sentinel の使用許諾契約の条項を確認して同意します。
8. ［*次へ*］を選択します。
9. ［ホスト名］および［ドメイン名］ページで、ホスト名とドメイン名を指定してから、［*ホスト名をループバック IP に割り当てる*］オプションが選択されていることを確認します。
10. ［*次へ*］を選択します。ホスト名の環境設定が保存されます。
11. 次のいずれかの操作を行います。
    - 現在のネットワーク接続設定を使用するには、［ネットワーク環境設定 II］ページで［*次の環境設定を使用する*］を選択します。
    - ネットワーク接続設定を変更するには、［*変更*］を選択し、目的の変更を行います。
12. ［*次へ*］を選択します。ネットワーク接続設定が保存されます。
13. 日付と時刻を設定して、［*次へ*］をクリックします。

    インストール後に NTP 環境設定を変更するには、アプライアンスのコマンドラインから YaST を使用します。WebYast を使用して日付と時刻を変更することはできますが、NTP の環境設定を変更することはできません。

    インストール直後に時刻が同期されていない場合は、次のコマンドを実行して NTP を再起動します。

```
rcntp restart
```

14 root のパスワードを設定して、［*次へ*］をクリックします。

15 Sentinel 管理者のパスワードを設定してから、［*次へ*］をクリックします。

16 コンソールでユーザ名とパスワードを入力して、アプライアンスにログインします。

ユーザ名のデフォルト値は root で、パスワードはステップ 14 で設定されたものです。

17 Sentinel サーバを停止します。

```
service sentinel stop
```

18 次のコマンドを入力して UI をリセットし、YaST での表示を整頓します。

```
reset
```

19 物理サーバにアプライアンスをインストールするには、次のコマンドを実行します。

/sbin/yast2 live-installer

システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

20 コンソールに表示されたアプライアンスの IP アドレスをメモします。

21 52 ページのセクション 5.5「アプライアンスのインストール後の環境設定」に従って手順を進めます。

## 5.4.2 コレクタマネージャのインストール

コレクタマネージャは、その最小ハードウェア要件を満たす Linux システム上に、アプライアンスとしてインストールすることができます。詳細については、12 ページのセクション 1.1.2「ハードウェア要件」を参照してください。

1 49 ページのセクション 5.4.1「Sentinel のインストール」のステップ 1 からステップ 14 を実行します。

2 コレクタマネージャが接続する Sentinel サーバのホスト名または IP アドレスを指定します。

3 Communication Server のポート番号を指定します。デフォルトのメッセージバスのポートは 61616 です。

指定された資格情報によってサーバへの接続が試行されます。入力された値が間違っていると、エラーが表示されます。

4 JMS ユーザ名を指定します。これは、コレクタマネージャのユーザ名です。デフォルトのユーザ名は collectormanager です。

5 JMS ユーザのパスワードを指定します。

6 ［*次へ*］をクリックします。

ユーザ名とパスワードは、Sentinel サーバにある /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。

7 パスワードを確認するには、activemqusers.properties ファイル内の次の行を確認します。

```
collectormanager=<password>
```

この例では、collectormanager はユーザ名であり、対応する値はパスワードです。

8 同意を求められたら、証明書に同意します。

9 [ *次へ* ] をクリックしてインストールを完了します。

インストールが完了したら、このアプライアンスが Sentinel コレクタマネージャであることと、IP アドレスを示すメッセージが表示されます。また、Sentinel サーバのユーザインタフェース IP アドレスも表示します。

### 5.4.3 相関エンジンのインストール

相関エンジンは、その最小ハードウェア要件を満たすシステム上に、アプライアンスとしてインストールすることができます。詳細については、12 ページのセクション 1.1.2「ハードウェア要件」を参照してください。

1 49 ページのセクション 5.4.1「Sentinel のインストール」のステップ 1 からステップ 14 を実行します。

2 相関エンジンが接続する Sentinel サーバのホスト名または IP アドレスを指定します。

3 Communication Server のポート番号を指定します。デフォルトのメッセージバスのポートは 61616 です。

4 JMS ユーザ名を指定します。これは、相関エンジンのユーザ名です。デフォルトのユーザ名は correlationengine です。

5 JMS ユーザのパスワードを指定します。

6 *[次へ]* をクリックします。

ユーザ名とパスワードは、Sentinel サーバにある /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。

7 パスワードを確認するには、activemqusers.properties ファイル内の次の行を確認します。

```
correlationengine=<password>
```

この例では、correlationengine はユーザ名であり、対応する値はパスワードです。

8 同意を求められたら、証明書に同意します。

9 [ *次へ* ] をクリックしてインストールを完了します。

インストールが完了したら、このアプライアンスが Sentinel 相関エンジンであることと、IP アドレスを示すメッセージが表示されます。また、Sentinel サーバのユーザインタフェース IP アドレスも表示します。

10 52 ページのセクション 5.5「アプライアンスのインストール後の環境設定」に従って手順を進めます。

## 5.5 アプライアンスのインストール後の環境設定

### 5.5.1 VMware Tools のインストール

Sentinel を VMware サーバ上で効果的に動作させるには、VMware Tools をインストールする必要があります。VMware Tools は、仮想マシンのオペレーティングシステムのパフォーマンスを向上させるユーティリティスイートです。仮想マシンの管理も改善されます。VMware Tools のインストールの詳細については、「VMware Tools for Linux Guests (https://www.vmware.com/support/ws55/doc/ws_newguest_tools_linux.html#wp1127177)」を参照してください。

VMware のマニュアルについての詳細は、『Workstation User's Manual (http://www.vmware.com/pdf/ws71_manual.pdf)』を参照してください。

### 5.5.2 アプライアンスの Web インタフェースへのログイン

アプライアンスの Web コンソールにログインしてソフトウェアを初期化するには、次の手順を実行します。

1. Web ブラウザを開いて https://<*IP_address*>:8443 にログインします。8443 は Sentinel サーバのデフォルトポートです。Sentinel の Web ページが表示されます。

   インストールが完了してサーバが再起動すると、アプライアンスの IP アドレスがアプライアンスコンソールに表示されます。

2. Sentinel アプライアンスでデータストレージおよびデータ収集の環境設定を行います。

   アプライアンスの環境設定の詳細については、『*NetIQ Sentinel 7.0.1 管理ガイド*』を参照してください。

3. アップデートの登録を行います。

   詳細については、54 ページのセクション 5.9「アップデートの登録」を参照してください。

## 5.6 WebYaST の環境設定

Sentinel アプライアンスのユーザインタフェースには WebYaST が備わっています。WebYaST とは、アプライアンスを制御するための Web ベースのリモートコンソールで、SUSE Linux Enterprise をベースにしています。WebYaST を使用して、Sentinel アプライアンスに対するアクセス、環境設定、監視を行います。次に、WebYaST の環境設定の手順について簡単に説明します。環境設定の詳細については、『*WebYaST User Guide* (http://www.novell.com/documentation/webyast/)』を参照してください。

1. Sentinel アプライアンスにログインします。
2. ［*アプライアンス*］をクリックします。
3. 54 ページのセクション 5.9「アップデートの登録」の説明にあるように、アップデートを受信する Sentinel サーバの環境設定を行います。
4. ［*次へ*］をクリックして、初期設定を完了します。

## 5.7 SMT でのアプライアンスの設定

インターネットに直接アクセスできない保護された環境でアプライアンスを実行する必要がある場合は、Subscription Management Tool (SMT) でアプライアンスを設定できます。これにより、Sentinel の最新バージョンが公開されると、アプライアンスを最新バージョンにアップグレードできます。SMT は、ノベルカスタマセンターと統合されたパッケージ代理システムで、主な Novell Customer Center 機能を提供します。


- 53 ページのセクション 5.7.1「前提条件」
- 54 ページのセクション 5.7.2「アプライアンスの設定」


### 5.7.1 前提条件

- 更新する Sentinel 用の Novell Customer Center 資格情報を Novell から入手します。資格情報の取得の詳細については、Novell サポート (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) に問い合わせてください。
- SMT をインストールするマシンに次のパッケージと共に SLES 11 SP1 がインストールされていることを確認します。
  - htmldoc
  - smt
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - pertl-DBIx-Migration-Director
  - perl-MIME-Lite
  - perl-Text-ASCIITable
  - smt-support
  - yast2-smt
  - yum-metadata-parser
  - createrepo
  - sle-smt-release-cd
  - sle-smt_en
  - perl-DBI
  - apache2-prefork
  - libapr1
  - perl-Data-ShowTable
  - perl-Net-Daemon
  - perl-Tie-IxHash
  - fltk
  - libapr-util1
  - perl-PIRPC
  - apache2-mod_perl
  - apache2-utils

- apache2
- perl-DBD-mysql

- SMT をインストールし、SMT サーバを設定します。詳細については、SMT のマニュアル (http://www.novell.com/documentation/smt11/) の以下に関するセクションを参照してください。
  - SMT のインストール
  - SMT サーバの設定
  - SMT でのインストールと更新リポジトリのミラーリング
- アプライアンスマシンに wget ユーティリティをインストールします。

### 5.7.2 アプライアンスの設定

SMT でのアプライアンスの設定については、Subscription Management Tool のマニュアルの「Configuring Clients to Use SMT (http://www.novell.com/documentation/smt11/smt_sle_11_guide/?page=/documentation/smt11/smt_sle_11_guide/data/smt_client.html)」を参照してください。

## 5.8 Web インタフェースによるサーバの停止と起動

次のように Web インタフェースを使用して、Sentinel サーバを起動および停止できます。

1. Sentinel アプライアンスにログインします。
2. ［*アプライアンス*］をクリックして、WebYaST を起動します。
3. ［*システムサービス*］をクリックします。
4. Sentinel サーバを停止するには、［*停止*］をクリックします。
5. Sentinel サーバを起動するには、［*開始*］をクリックします。

## 5.9 アップデートの登録

1. Sentinel アプライアンスにログインします。
2. ［*アプライアンス*］をクリックして、WebYaST を起動します。
3. ［*登録*］をクリックします。
4. アップデートを受信する電子メール ID を指定してから、システム名およびアプライアンス登録コードを指定します。
5. ［*保存*］をクリックします。

# 6 インストールのトラブルシューティング

このセクションでは、インストール時に発生する可能性があるいくつかの問題とその解決方法について説明します。


- 55 ページのセクション 6.1「ネットワーク接続が不正なためにインストールが失敗する」
- 55 ページのセクション 6.2「イメージを作成したコレクタマネージャまたは相関エンジンの UUID が作成されない」


## 6.1 ネットワーク接続が不正なためにインストールが失敗する

最初のブート時に、インストーラでネットワーク設定が不正であることを検出すると、エラーメッセージが表示されます。ネットワークが使用できない場合、アプライアンスへの Sentinel のインストールは失敗します。

この問題を解決するには、ネットワークを正しく設定します。環境設定を確認するには、有効な IP アドレスを返す ipconfig コマンドと、有効なホスト名を返す hostname -f コマンドを使用します。

## 6.2 イメージを作成したコレクタマネージャまたは相関エンジンの UUID が作成されない

コレクタマネージャサーバのイメージを作成し ( たとえば、ZENworks イメージングを使用 )、別のマシンにそのイメージを復元する場合。Sentinel はコレクタマネージャの新しいインスタンスを一意的に識別しません。これは、UUID が重複しているために発生します。

新しくインストールしたコレクタマネージャのシステムで次の手順を実行し、新しい UUID を生成する必要があります。

1. /var/opt/novell/sentinel/data フォルダにある host.id または sentinel.id ファイルを削除します。
2. コレクタマネージャを再起動します。

   コレクタマネージャが自動的に UUID を生成します。

# 7 次に行う作業

Sentinel をインストールした後は、Sentinel の環境設定について説明した次の 2 つのガイドを参照してください。『*NetIQ Sentinel 7.0.1 管理ガイド*』および『*NetIQ Sentinel 7.0.1 ユーザガイド*』。

『管理ガイド』には、管理権限を持っているユーザのみが実行できる作業の設定情報が記載されています。例 :

- 「ユーザと役割の設定」
- 「データストレージの設定」
- 「データ収集の設定」
- 「分散環境でのイベントの検索とレポート」

これらの作業およびその他の管理作業の詳細 については、『*NetIQ Sentinel 7.0.1 管理ガイド*』を参照してください。

『ユーザガイド』には、Sentinel でユーザが実行する作業に役立つ説明が記載されています。例 :

- 「イベントの検索」
- 「データのトレンドの分析」
- 「レポーティング」
- 「インシデントの設定」

これらの作業およびその他のユーザ作業の詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』を参照してください。

また、イベントの分析、相関ルールを使用したデータの追加、ベースラインの設定、情報に対するワークフローの設定などを行うよう、Sentinel を設定することができます。Sentinel のこれらの機能を設定する際は、『*NetIQ Sentinel 7.0.1 管理ガイド*』の情報を参考にしてください。

# II 設定

Sentinel のインストール後、環境内で実行できるように Sentinel を設定します。

# 8 Sentinel Web インタフェースへのアクセス

Sentinel のインストール後、Sentinel Web インタフェースにログインして管理作業を実行し、データを収集するように Sentinel を設定します。

1. Web ブラウザを開いて https://<*IP_address*>:8443 にログインします。8443 は Sentinel サーバのデフォルトポートです。
2. ( 条件による )Sentinel への初回ログイン時に、証明書への同意を求められたら同意します。

   証明書に同意すると、Sentinel のログインページが表示されます。
3. Sentinel 管理者のユーザ名とパスワードを指定します。
4. [ *ログイン* ] をクリックします。

   NetIQ Sentinel の Web インタフェースが表示されます。

# 9 新たな Sentinel コンポーネントの追加

デフォルトでは、Sentinel には Syslog Connector、Syslog Collector、および各種監査コネクタと Novell 製品コレクタがインストールおよび設定されています。次のセクションでは、追加のコネクタおよびコレクタのインストールおよび設定方法を説明します。


- 63 ページのセクション 9.1「コレクタとコネクタのインストール」
- 64 ページのセクション 9.2「新たなコレクタとコネクタの追加」


## 9.1 コレクタとコネクタのインストール

デフォルトでは、Sentinel 7 をインストールすると、リリースされているすべてのコレクタおよびコネクタがインストールされます。Sentinel 7 の後に新しいコレクタおよびコネクタがリリースされた場合、コレクタおよびコネクタのファイルをインストールしてから、これらの設定を行う必要があります。


- 63 ページのセクション 9.1.1「コレクタのインストール」
- 64 ページのセクション 9.1.2「コネクタのインストール」


### 9.1.1 コレクタのインストール

1. Sentinel プラグインの Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) から、正しいコレクタをダウンロードします。
2. https://<*IP address*>:8443 で Sentinel Web インタフェースにログインします。8443 は、Sentinel サーバのデフォルトポートです。
3. ツールバーで［*アプリケーション*］をクリックしてから、［*アプリケーション*］をクリックします。
4. ［*コントロールセンターの起動*］をクリックして Sentinel コントロールセンターを起動します。
5. ツールバーで、［*イベントソースの管理*］>［*ライブビュー*］の順にクリックし、［*ツール*］>［*プラグインのインポート*］の順にクリックします。
6. ステップ 1 でダウンロードしたコレクタファイルをブラウズして選択してから、［*次へ*］をクリックします。
7. 残りのプロンプトに従った後、［*終了*］をクリックします。

コレクタを設定するには、Sentinel プラグインの Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) にある、固有のコレクタのマニュアルを参照してください。

### 9.1.2 コネクタのインストール

1 Sentinel プラグインの Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) から、正しいコネクタをダウンロードします。

2 https://<*IP address*>:8443 で Sentinel Web インタフェースにログインします。8443 は、Sentinel サーバのデフォルトポートです。

3 ツールバーで［*アプリケーション*］をクリックしてから、［*アプリケーション*］をクリックします。

4 ［*コントロールセンターの起動*］をクリックして Sentinel コントロールセンターを起動します。

5 ツールバーで、［*イベントソースの管理*］>［*ライブビュー*］の順に選択し、［*ツール*］>［*プラグインのインポート*］の順にクリックします。

6 ステップ 1 でダウンロードしたコネクタファイルをブラウズして選択してから、［*次へ*］をクリックします。

7 残りのプロンプトに従った後、［*終了*］をクリックします。

コネクタを設定するには、Sentinel プラグインの Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) にある、固有のコネクタのマニュアルを参照してください。

## 9.2 新たなコレクタとコネクタの追加


- 64 ページのセクション 9.2.1「新たなコレクタの追加」
- 65 ページのセクション 9.2.2「新たなコネクタの追加」


### 9.2.1 新たなコレクタの追加

新たなコレクタを追加して、他のソースからのデータを正規化することができます。

1 https://<*IP address*>:8443 で Sentinel Web インタフェースにログインします。8443 は、Sentinel サーバのデフォルトポートです。

2 ツールバーで［*アプリケーション*］をクリックしてから、［*アプリケーション*］をクリックします。

3 ［*コントロールセンターの起動*］をクリックして Sentinel コントロールセンターを起動します。

4 ツールバーで、［*イベントソースの管理*］>［*ライブビュー*］の順に選択します。

5 Collector Manager を右クリックし、［*Collector の追加*］をクリックします。

6 ［*ベンダ名*］の欄からコレクタを選択してから、［*次へ*］をクリックします。

7 これ以降は、コレクタによってフィールドが異なるため、コレクタを設定するには固有のコレクタのマニュアルに従う必要があります。

   コレクタのマニュアルは、Sentinel プラグインの Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) にあります。

### 9.2.2 新たなコネクタの追加

新たなコネクタを追加して、他のソースから情報を収集することができます。

1. https://<*IP address*>:8443 で Sentinel Web インタフェースにログインします。8443 は、Sentinel サーバのデフォルトポートです。
2. ツールバーで［*アプリケーション*］をクリックしてから、［*アプリケーション*］をクリックします。
3. ［*コントロールセンターの起動*］をクリックして Sentinel コントロールセンターを起動します。
4. ツールバーで、［*イベントソースの管理*］>［*ライブビュー*］の順に選択します。
5. 新たなコネクタを追加するコレクタを右クリックしてから、［*コネクタの追加*］をクリックします。
6. ［*名前*］の欄から目的のコネクタを選択してから、［*次へ*］をクリックします。
7. これ以降は、コネクタによってフィールドが異なるため、コネクタを設定するには固有のコネクタのマニュアルに従う必要があります。

   コネクタのマニュアルは、Sentinel プラグインの Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) にあります。

# 10 データの管理



## 10.1 ディレクトリ構造

デフォルトでは、Sentinel のディレクトリは次の場所にあります。

- データファイルは、/var/opt/novell/sentinel/data ディレクトリおよび /var/opt/novell/sentinel/3rdparty ディレクトリにあります。
- 実行可能ファイルとライブラリは、次の場所にあります。
  - /opt/novell/sentinel/bin
  - /opt/novell/sentinel/setup
  - /opt/novell/sentinel/3rdparty
- ログファイルは、/var/opt/novell/sentinel/log ディレクトリにあります。
- 環境設定ファイルは、/etc/opt/novell/sentinel ディレクトリにあります。
- プロセス ID (PID) ファイルは、/var/run/sentinel/server.pid ディレクトリにあります。

  PID を使用すると、管理者は Sentinel サーバの親プロセスを識別し、プロセスを監視または終了することができます。

## 10.2 ストレージの考慮事項

Sentinel のデータファイルを格納する際は、実行ファイル、環境設定ファイル、およびオペレーティングシステムファイルとは別のパーティションにデータファイルを格納するようにしてください。データを別のパーティションに格納する利点は、ファイルセットのイメージの作成と、破損の際の回復が容易になる点です。また、容量の小さいファイルシステムのほうが効率的であるため、システム全体のパフォーマンスも向上します。詳細については、「「Disk partitioning ( パーティション )」(http://en.wikipedia.org/wiki/Disk_partitioning#Benefits_of_multiple_partitions)」を参照してください。

以下のインストールの種類によって、Sentinel を複数のパーティションにインストールするか、または単一のパーティションにインストールするかを決定できます。

- スタンドアロンインストール
- アプライアンスインストール

### 10.2.1 スタンドアロンインストールでのパーティションの使用

スタンドアロンインストールとして Sentinel をインストールする場合、Sentinel をインストールする前にオペレーティングシステムのパーティションのレイアウトを変更できます。管理者は 67 ページのセクション 10.1「ディレクトリ構造」で説明されているディレクトリ構造に基づいて、適切なディレクトリに目的のパーティションを作成およびマウントする必要があります。インストーラを実行すると Sentinel は事前に作成されたディレクトリにインストールされ、複数のパーティションにわたってインストールされます。

---

**NOTE**:

- インストーラの実行中に --location オプションを使用して、デフォルトのディレクトリ以外の場所にファイルを格納するよう指定できます。--location オプションに渡す値は、ディレクトリパスの前に付加されます。たとえば、「--location=/foo」を指定すると data ディレクトリは /foo/var/opt/novell/sentinel/data、config ディレクトリは /foo/etc/opt/novell/sentinel/config となります。
- --location オプションでは、ファイルシステムのリンク ( ソフトリンクなど ) は使用できません。

---

### 10.2.2 アプライアンスインストールでのパーティションの使用

アプライアンスインストールを使用して Sentinel をインストールする場合、Sentinel をインストールする前にオペレーティングシステムを再設定することはできません。これは、オペレーティングシステムと共に Sentinel がインストールされるためです。ただし、YaST ツールを使用して、アプライアンスにパーティションを追加し、新しいパーティションにディレクトリを移動させることはできます。

次の手順で新しいパーティションを作成し、データファイルを元のディレクトリから新しく作成したパーティションに移動させます。

1. Sentinel に root としてログインします。
2. 次のコマンドを実行して、アプライアンス上の Sentinel を停止させます。

   /etc/init.d/sentinel stop
3. 次のコマンドを指定して、novell ユーザに変更します。

   su -novell
4. /var/opt/novell/sentinel のディレクトリの内容を一時的にどこかの場所に移動します。
5. root ユーザに変更します。
6. 次のコマンドを入力して、YaST2 コントロールセンターにアクセスします。

   `yast`
7. *[システム] > [パーティショナ]* の順に選択します。
8. 警告を確認して［*はい*］を選択し、新しい未使用パーティションを追加します。
9. /var/opt/novell/sentinel に新しいパーティションをマウントします。
10. 次のコマンドを指定して、novell ユーザに変更します。

    su -novell
11. ディレクトリの内容を一時保存先 ( ステップ 4 で保存した場所 ) から、新しいパーティション内の /var/opt/novell/sentinel に戻します。

**12** root ユーザに変更します。

**13** 次のコマンドを実行して、Sentinel アプライアンスを再起動します。

/etc/init.d/sentinel start

# 11 導入後直ちに使用可能なコンテンツの設定

Sentinel には、分析に関する多数のニーズに合わせて、導入後直ちに使用可能なさまざまなコンテンツが同梱されています。このようなコンテンツの多くはプレインストールされた Sentinel コアソリューションパックに含まれています。詳細については、『「Novell Sentinel 7.0.1 ユーザガイド」』の「*Using Solution Packs ( ソリューションパックの使用 )*」を参照してください。・

ソリューションパックでは、コンテンツをコントロールまたはポリシーセットに分類およびグループ化することができ、それらが 1 つのユニットとして扱われます。この導入後直ちに使用可能なコンテンツを提供するために、Sentinel コアソリューションパックのコントロールはプレインストールされていますが、これらのコントロールは Sentinel Web UI を使用して形式的に実装またはテストする必要があります。

Sentinel の実装が設計どおりに機能していることをある程度厳密に確認する場合は、ソリューションパックに組み込まれた形式的検証プロセスを使用できます。この検証プロセスでは、他のソリューションパックのコントロールの実装とテストを行う場合と全く同じように、Sentinel コアコントロールを実装およびテストします。このプロセスの一環として、実装担当者とテスト担当者が作業を完了したことを検証します。次に、これらの検証が監査証跡に含められ、特定のコントロールが正しく展開されたことを確認できます。

検証プロセスは、ソリューションマネージャを使用して実施できます。詳細については、『「Novell Sentinel 7.0.1 ユーザガイド」』の「*Installing and Managing Solution Packs ( ソリューションパックのインストールと管理 )*」を参照してください。・

# 12 時刻の設定

イベントの時刻は、Sentinel におけるイベントの処理には不可欠のものです。これはリアルタイム処理だけでなく、レポートや監査のためにも重要です。

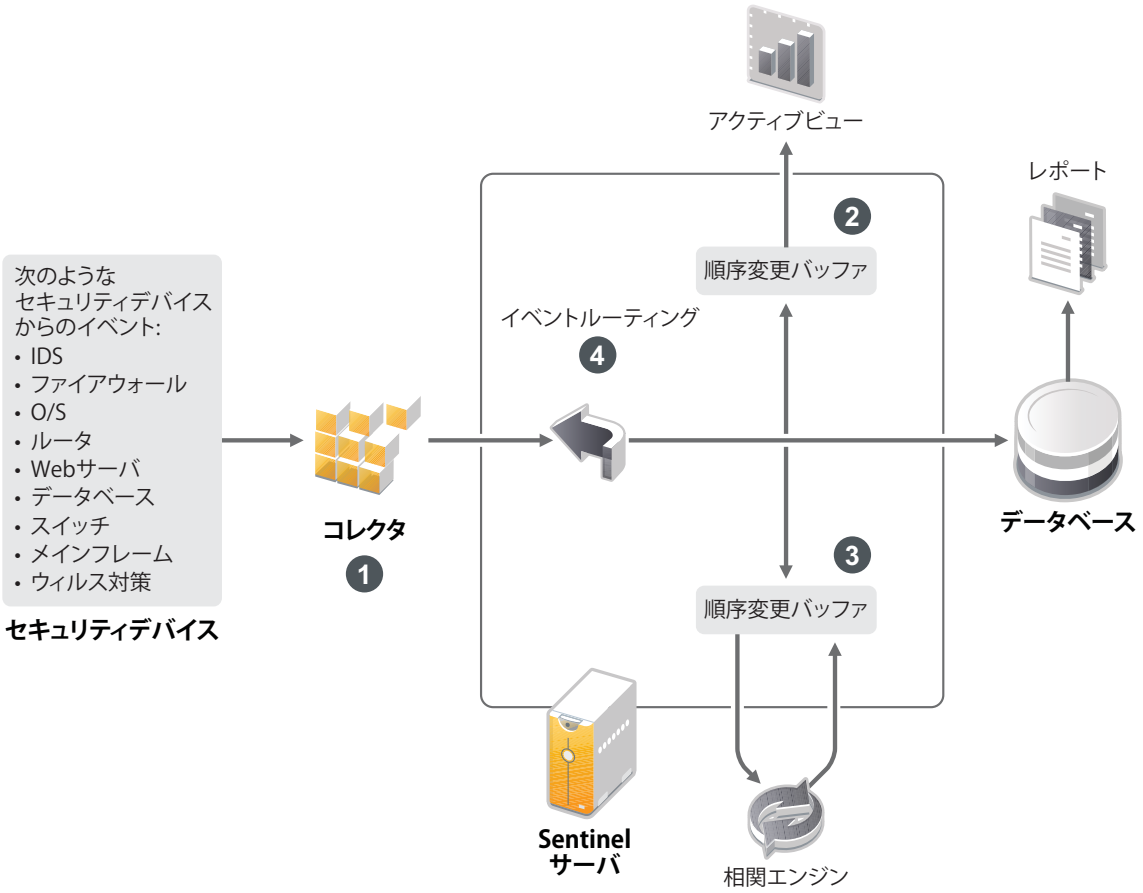


## 12.1 Sentinel における時刻について

Sentinel は分散システムであり、ネットワークのさまざまな部分に配置できる複数のプロセスで構成されています。また、デバイスによって遅延が発生する可能性があります。これに対応するために、Sentinel プロセスは、イベントを処理する前に、イベントの順序を変更して時間順に並べられたストリームにします。

次の図は、Sentinel がこれをどのように処理するのかを示しています。

*図 12-1　Sentinel の時刻*




1. デフォルトでは、イベント時刻がコレクタマネージャの時刻に設定されます。理想的な時刻は、デバイスの時刻です。したがって、デバイス時刻が利用可能で、正確であり、コレクタによって適切に解析される場合は、イベント時刻をデバイス時刻に設定することが最適です。
2. イベントは 30 秒間隔でソートされ、アクティブビューで確認できます。デフォルトでは、サーバ時刻から前後 5 分の範囲内のタイムスタンプを有するイベントは、通常通り処理されます。タイムスタンプが 5 分後よりも後のイベントは、アクティブビューには表示されませんが、イベントストアには挿入されます。タイムスタンプが 5 分前よりも前で、そして 24 時間前までのイベントは、チャートには表示されますが、チャートのイベントデータには表示されません。これらのイベントをイベントストアから取得するには、ドリルダウン操作が必要です。
3. イベント時刻がサーバ時刻よりも 30 秒を超えて古い場合、相関エンジンはイベントを処理しません。
4. イベント時刻がコレクタマネージャ時刻 ( 正しい時刻 ) よりも 5 分を超えて古い場合、イベントはイベントストアに直接ルーティングされます。

## 12.2 Sentinel における時刻の設定

相関エンジンは、時間順に並べられたイベントのストリームを処理し、イベント内のパターンおよびストリーム内の時系列パターンを検出します。しかし、時々、イベントを生成するデバイスについてログメッセージに時刻が組み込まれないことがあります。Sentinel で時刻を正しく取り扱えるように設定するには、次の 2 つの方法があります。

- コレクタマネージャで NTP を設定し、イベントソースマネージャのイベントソース上で［*信頼イベントソース時刻*］の選択を解除します。Sentinel は、イベント時刻のソースとしてコレクタマネージャを使用します。
- イベントソースマネージャのイベントソース上で［*信頼イベントソース時刻*］を選択します。Sentinel は、ログメッセージの時刻を正しい時刻として使用します。

この設定をイベントソース上で変更するには :

1. ［イベントソースの管理］にログインします。

   詳細については、『「Novell Sentinel 7.0.1 管理ガイド」』の「*Accessing Event Source Management ( イベントソース管理へのアクセス )*」を参照してください。
2. 時刻の設定を変更するイベントソースを右クリックしてから、［*編集*］を選択します。
3. ［*全般*］タブの下の［*Trust Event Source*］オプションを選択または選択解除します。
4. ［OK］*をクリックして変更内容を保存します。*

## 12.3 タイムゾーンの処理

分散環境では、タイムゾーンの処理が複雑になる場合があります。たとえば、あるタイムゾーンにイベントソースがあり、別のタイムゾーンにコレクタマネージャがあり、また別のタイムゾーンにバックエンドの Sentinel サーバがあり、さらに別のタイムゾーンでクライアントがデータを表示している場合などです。さらに夏時間や、設定されているタイムゾーンをレポートしないイベントソース ( すべての Syslog ソースなど ) を考慮すると、処理を必要とする問題は多くあります。Sentinel は、イベントが実際に発生した時刻を正しく示し、これらのイベントを同じタイムゾーンまたは別のタイムゾーンの他のイベントと比較することを可能にする柔軟性を備えています。

一般的に、イベントソースがタイムスタンプをレポートする方法は 3 通りあります。

- イベントソースが UTC で時刻をレポートする場合。たとえば、Windows イベントログの標準的なイベントはすべて、常に UTC でレポートされます。
- イベントソースがローカル時刻でレポートを行い、タイムスタンプにタイムゾーン情報が含まれている場合。たとえば、RFC3339 に従ってタイムスタンプを構成するイベントソースはすべて、オフセットとしてタイムゾーンを含みます。他のソースはアメリカ / ニューヨークなどの長いタイムゾーン ID、または EST などの短いタイムゾーン ID をレポートするため、不一致や不適切な解決などによる問題が発生する場合があります。
- イベントソースがローカル時刻でレポートし、タイムゾーン情報を含まない場合。残念ながら、とてもよく使われる Syslog フォーマットはこの形です。

最初の方法では、イベントが発生した絶対 UTC 時刻を計算できるため ( 時刻同期プロトコルが使用されていると想定 )、そのイベントの時刻を他の世界中のイベントソースと容易に比較できます。ただし、イベントが発生したときのローカル時刻は自動的には判断できません。このため、Sentinel では、イベントソースのタイムゾーンを手動で設定できるようになっています。これは、イベント

ソースマネージャでイベントソースノードを編集して、適切なタイムゾーンを指定することにより可能です。この情報は［デバイスのイベント時刻］や［イベント時刻］の計算には影響しませんが、［オブザーバのタイムゾーン］フィールドに取り込まれ、［オブザーバのタイムゾーンの時間］などの多様な［オブザーバのタイムゾーン］フィールドの計算に使用されます。これらのフィールドは、常にローカル時刻で示されます。

2 つめの方法は、いろいろな意味で最もシンプルです。長い形式のタイムゾーン ID またはオフセットが使用されている場合、容易に UTC に変換して絶対的な標準 UTC 時刻 (［デバイスのイベント時刻］に格納される ) を取得できますが、ローカル時刻の［オブザーバのタイムゾーン］フィールドを計算するのも容易です。短い形式のタイムゾーン ID が使用されている場合、不一致が発生する可能性があります。

3 つめの方法には注意が必要です。Sentinel が UTC 時刻を正しく計算できるよう、影響を受けるすべてのソースのイベントソースタイムゾーンを管理者が手動で設定する必要があるからです。イベントソースマネージャでイベントソースノードを編集してタイムゾーンを正しく指定していない場合、［デバイスのイベント時刻］( および、多くの場合は［イベント時刻］) が正しくない可能性があり、［オブザーバのタイムゾーン］および関連するフィールドも正しくない場合があります。

一般的に、特定のイベントソース ( たとえば、Microsoft Windows など ) 用のコレクタは、イベントソースからのタイムスタンプの形式が判明しているため、それに応じて調整を行います。イベントソースがローカル時刻でレポートし、タイムスタンプに常にタイムゾーンが含まれているのでない限り、イベントソースマネージャでイベントソースノードすべてに対して手動でタイムゾーンを設定することをお勧めします。

イベントソースからのタイムスタンプ情報は、コレクタおよびコレクタマネージャ上で処理されます。［デバイスのイベント時刻］および［イベント時刻］は UTC として格納され、［オブザーバのタイムゾーン］フィールドはイベントソースのローカル時刻の文字列として格納されます。この情報はコレクタマネージャから Sentinel サーバに送信され、イベントストア内に格納されます。コレクタマネージャおよび Sentinel サーバが配置されたタイムゾーンは、このプロセスにも格納されるデータにも影響しません。ただし、クライアントが Web ブラウザでイベントを確認する場合、UTC の［イベント時刻］は Web ブラウザによってローカル時刻に変換されます。そのため、クライアントには、すべてのイベントがローカルのタイムゾーンで示されます。ユーザがソースのローカル時刻を知りたい場合は、［オブザーバのタイムゾーン］フィールドで詳細を確認できます。

# 13 ライセンス情報

このセクションでは Sentinel の各種ライセンスについて説明し、ライセンスの管理方法についての情報を提供します。


- 77 ページのセクション 13.1「Sentinel ライセンスについて」
- 78 ページのセクション 13.2「ライセンスキーの追加」


## 13.1 Sentinel ライセンスについて

Sentinel で使用できるライセンスは数種類あります。デフォルトでは、Sentinel には評価版ライセンスが付帯しています。


- 77 ページのセクション 13.1.1「評価版ライセンス」
- 78 ページのセクション 13.1.2「エンタープライズライセンス」


### 13.1.1 評価版ライセンス

Sentinel のデフォルトライセンスにより、90 日間の評価期間中、すべての Sentinel エンタープライズ版機能を使用できます。評価版ライセンスで稼働しているシステムでは、Web インタフェース上に、一時ライセンスキーが使用されていることが示されます。また、機能の残り日数および、フルライセンスへのアップグレード方法も表示されます。

---

**NOTE**: システムの有効期限は、システム内で最も古いデータに基づきます。古いイベントをシステムで復元すると、それに従って有効期限が調整されます。

---

90 日の評価期間後、ほとんどの機能は無効になりますが、ログインしてエンタープライズライセンスキーを使用するようにシステムを更新することはできます。

エンタープライズライセンスにアップグレードすると、すべての機能が復元されます。機能の中断を防ぐには、期限までにシステムをエンタープライズライセンスでアップグレードする必要があります。

### 13.1.2 エンタープライズライセンス

Sentinel を購入すると、お客様向けポータルから、ライセンスキーを受け取ります。購入したライセンスに応じて、ライセンスキーによって特定の機能、データ収集レート、およびイベントソースが有効になります。ライセンスキーでは強制されない追加のライセンス条件が存在する可能性があるため、使用許諾契約は十分に確認してください。

ライセンスを変更する場合は、アカウントマネージャにお問い合わせください。システムにライセンスキーを追加するには、78 ページのセクション 13.2.1「Web インタフェースを使用したライセンスキーの追加」を参照してください。

## 13.2 ライセンスキーの追加

**NOTE**: ライセンスを追加、表示、または削除するには、管理者権限が必要です。

ライセンスキーは、Web インタフェースを使用するか、またはコマンドラインから追加できます。


- 78 ページのセクション 13.2.1「Web インタフェースを使用したライセンスキーの追加」
- 78 ページのセクション 13.2.2「コマンドラインによるライセンスキーの追加」


### 13.2.1 Web インタフェースを使用したライセンスキーの追加

1. 管理者として Sentinel Web インタフェースにログインします。
2. ページの左上にある［*バージョン情報*］リンクをクリックします。
3. ［*ライセンス*］タブをクリックします。
4. ［ライセンス］セクションで、［*ライセンスの追加*］をクリックします。
5. ［キー］フィールドでライセンスキーを指定します。ライセンスを指定すると、［プレビュー］セクションに次の情報が表示されます。

   **機能 :** このライセンスで使用できる機能。

   **ホスト名 :** このフィールドは、NetIQ の内部利用に限定されます。

   **シリアル :** このフィールドは、NetIQ の内部利用に限定されます。

   **EPS:** ライセンスキーに組み込まれたイベントレート。このレートを超えると、Sentinel は警告を発しますが、データの収集は続行します。

   **有効期限 :** ライセンスの期限。機能を中断させないよう、期限より前に有効なライセンスキーを指定する必要があります。
6. *［保存］*をクリックします。

### 13.2.2 コマンドラインによるライセンスキーの追加

softwarekey.sh スクリプトを使用して、コマンドラインからライセンスを追加できます。

1. Sentinel サーバに root としてログインします。
2. /opt/novell/sentinel/bin ディレクトリに移動します。
3. 次のコマンドを入力して、novell ユーザに変更します。

su novell

4 次のコマンドを指定して、softwarekey.sh スクリプトを実行します。

```
./softwarekey.sh
```

5 「1」と入力してライセンスキーを挿入します。

6 ライセンスキーを指定して、<Enter> を押します。

# 14 高可用性のための Sentinel の環境設定

Sentinel は、高可用性環境で動作するようテストおよび認定されており、障害復旧アーキテクチャをサポートします。NetIQ コンサルティングおよび NetIQ パートナーは、Sentinel の高可用性および障害復旧の実装を支援します。

Sentinel サーバで高可用性を実現するには、以下が必要です。

- 冗長化およびクラスタ化された Sentinel ノード。
- 共有データストレージへのアクセス。
- 不具合のあるノードから別のノードに透過的に移行するのに使用できる仮想 IP アドレス。
- クラスタソリューションに定義されたポリシーに基づいて、アプリケーションを起動、停止、および監視するスクリプト。Linux Enterprise High Availability システム上では、Cluster Resource Agents や LSB init スクリプトなどのクラスタソリューションを使用できます。

高可用性を実現するパッケージは、数多く公開されています。Sentinel に対しては、*SUSE Linux Enterprise High Availability (HA) Extension* (http://www.novell.com/products/highavailability/)、共有ストレージ RAID ドライブ、およびカスタムスクリプトがテストされています。このアーキテクチャはデータセンター間で複製でき、Sentinel サーバ、コレクタマネージャ、およびコレクタなどすべてが使用できるようになります。

使用できるデバイスは多岐にわたるため、イベントソースの高可用性は個別に検討する必要があります。

# III Sentinel のアップグレード

# 15 Sentinel サーバのアップグレード

1 環境設定のバックアップを行った後、ESM エクスポートを作成します。

データのバックアップの詳細については、「「Backing Up and Restoring Data ( データのバックアップと復元 )」」を参照してください。これは『*NetIQ Sentinel 7.0.1 Administration Guide*』にあります。

2 ノベル製品ダウンロードのサイト (http://download.novell.com) から最新のインストーラをダウンロードします。

3 Sentinel をアップグレードするサーバに roo t としてログインします。

4 次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

```
tar xfz <install_filename>
```

<*install_filename*> は、実際のインストールファイル名に置き換えます。

5 インストールファイルを抽出したディレクトリに移動します。

6 次のコマンドを指定して、Sentinel をアップグレードします。

```
./install-sentinel
```

7 指定の言語でインストールを進めるには、言語の横の番号を選択します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

8 エンドユーザの使用許諾契約を読み、「yes」または「y」と入力して契約に同意し、インストールを続行します。

9 インストールスクリプトで、古いバージョンの製品が存在していることが検出され、製品をアップグレードするかどうかを指定するよう求められます。「n」を押すと、インストールは終了します。アップグレードを続行するには、「y」を押します。

すべての RPM パッケージのインストールが開始されます。このインストールが完了するまで数秒かかることがあります。

10 ( 条件による ) コレクタマネージャシステムをアップグレードするには、89 ページの第 17 章「コレクタマネージャのアップグレード」を参照してください。

11 ( 条件による ) 相関エンジンシステムをアップグレードするには、91 ページの第 18 章「相関エンジンのアップグレード」を参照してください。

# 16 Sentinel アプライアンスのアップグレード

この手順では、Sentinel アプライアンス、およびコレクタマネージャアプライアンスと相関エンジンアプライアンスのアップグレードについてご説明します。

1 Sentinel アプライアンスに管理者の役割を持つユーザとしてログインします。

2 ***Sentinel アプライアンスをアップグレードする場合は***、［*アプライアンス*］をクリックして WebYaST を起動します。

3 ***コレクタマネージャまたは相関エンジンアプライアンスをアップグレードする場合は***、ポート 54984 を使用しているコレクタマネージャか相関エンジンのコンピュータの URL を指定して、WebYaST を起動します。

4 環境設定のバックアップを行った後、ESM エクスポートを作成します。

   データのバックアップの詳細については、「「Backing Up and Restoring Data ( データのバックアップと復元 )」」を参照してください。これは『*NetIQ Sentinel 7.0.1 Administration Guide*』にあります。

5 ( 条件による ) アプライアンスの自動更新をまだ登録していない場合は、登録します。

   詳細については、54 ページのセクション 5.9「アップデートの登録」を参照してください。

   アプライアンスが登録されていない場合、黄色の警告が表示され、アプライアンスが登録されていないことが示されます。

6 アップデートがあるかどうかを確認するには、［*更新*］をクリックします。

   利用可能な更新が表示されます。

7 更新を選択して適用します。

   更新が完了するまで数分かかる場合があります。更新が成功すると、WebYaST のログインページが表示されます。

   アプライアンスをアップグレードする前に、WebYaST は Sentinel サービスを自動的に停止します。アップグレードが完了した後で、このサービスを手動で再開する必要があります。

8 Web インタフェースを使用して Sentinel サービスを再開します。

   詳細については、54 ページのセクション 5.8「Web インタフェースによるサーバの停止と起動」を参照してください。

# 17 コレクタマネージャのアップグレード

1 環境設定のバックアップを行い、ESM エクスポートを作成します。

   詳細については、『*NetIQ Sentinel 7.0.1 Administration Guide*』の「「Backing Up and Restoring Data」」を参照してください。

2 Sentinel の Web インタフェースに管理者の役割を持つユーザとしてログインします。

3 ［*ダウンロード*］を選択します。

4 コレクタマネージャのインストーラセクションで［*インストーラのダウンロード*］をクリックします。

   ウィンドウが表示されたら、インストーラファイルを実行するか、ローカルマシンに保存するかを選択します。

5 ファイルを保存します。

6 ファイルを一時的な場所にコピーします。

7 ファイルの内容を抽出します。

8 次のスクリプトを実行します。

   ./install-cm

9 画面の説明に従って、インストールを完了します。

# 18 相関エンジンのアップグレード

1 環境設定のバックアップを行い、ESM エクスポートを作成します。

   詳細については、『*NetIQ Sentinel 7.0.1 Administration Guide*』の「「Backing Up and Restoring Data」」を参照してください。

2 Sentinel の Web インタフェースに管理者の役割を持つユーザとしてログインします。

3 ［*ダウンロード*］を選択します。

4 相関エンジンのインストーラセクションで［*インストーラのダウンロード*］をクリックします。

   ウィンドウが表示されたら、インストーラファイルを実行するか、ローカルマシンに保存するかを選択します。

5 ファイルを保存します。

6 ファイルを一時的な場所にコピーします。

7 ファイルの内容を抽出します。

8 次のスクリプトを実行します。

   ./install-ce

9 画面の説明に従って、インストールを完了します。

# 19 Sentinel プラグインのアップグレード

新規および更新された Sentinel プラグインは、Sentinel プラグインの Web サイト (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) に頻繁にアップロードされます。最新のバグフィックス、マニュアルの更新、およびプラグインの拡張機能を取得するには、プラグインの最新バージョンをダウンロードします。プラグインのインストールやアップグレードについては、それぞれのプラグインのマニュアルを参照してください。

# IV 移行

# 20 サポートされる移行のシナリオ

Sentinel の本リリースでは、サポートされている移行シナリオはありません。移行やアップグレードではなく、Sentinel の新規インストールを実行する必要があります。ただし、データを移行するツールはまもなくリリースされます。

詳細については、23 ページの第 2 章「Sentinel のインストール」を参照してください。

# 21 次に行う作業

Sentinel をインストールした後は、Sentinel の環境設定について説明した次の 2 つのガイドを参照してください。『*NetIQ Sentinel 7.0.1 管理ガイド*』および『*NetIQ Sentinel 7.0.1 ユーザガイド*』。

『管理ガイド』には、管理権限を持っているユーザのみが実行できる作業の設定情報が記載されています。例 :

- 「ユーザと役割の設定」
- 「データストレージの設定」
- 「データ収集の設定」
- 「分散環境でのイベントの検索とレポート」

これらの作業およびその他の管理作業の詳細については、『*NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1 管理ガイド)*』を参照してください。

『ユーザガイド』には、Sentinel でユーザが実行する作業に役立つ説明が記載されています。例 :

- 「イベントの検索」
- 「データのトレンドの分析」
- 「レポーティング」
- 「インシデントの設定」

これらの作業およびその他のユーザ作業の詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』を参照してください。

また、イベントの分析、相関ルールを使用したデータの追加、ベースラインの設定、情報に対するワークフローの設定などを行うよう、Sentinel を設定することができます。Sentinel のこれらの機能を設定する際は、『*NetIQ Sentinel 7.0.1 管理ガイド*』の情報を参考にしてください。

# V アンインストール中

Sentinel をアンインストールするには、次の作業を実行します。

# 22 Sentinel のアンインストール

Sentinel のインストールを削除するのに役立つアンインストーラスクリプトを使用できます。ログファイルを含め、複数のファイルは保持され、必要に応じて手動で削除することができます。新規のインストールを実行する前に、以前のインストールのファイルまたはシステム設定が残らないようにするために、次の手順をすべて実行する必要があります。

**WARNING**: これらの手順では、オペレーティングシステムの設定やファイルを変更します。システム設定やファイルの変更方法に精通したユーザでない場合は、システム管理者に問い合わせてください。



## 22.1 Sentinel サーバのアンインストール

1. Sentinel サーバに root としてログインします。

   **NOTE**: root ユーザとしてインストールを実行している場合、root 以外のユーザで Sentinel サーバをアンインストールすることはできません。ただし、root 以外のユーザがインストールしている場合は、root 以外のユーザで Sentinel サーバをアンインストールできます。

2. 次のディレクトリにアクセスします。

   `/opt/novell/sentinel/setup/`

3. 次のコマンドを実行します。

   `./uninstall-sentinel`

4. アンインストールを続行するかどうか再確認を求められたら、「y」を押します。

   スクリプトはまずサービスを停止し、その後に削除を実行します。

## 22.2 リモートのコレクタマネージャまたは相関エンジンのアンインストール

1. root としてログインします。

**NOTE**: root ユーザとしてインストールを実行している場合、root 以外のユーザでリモートコレクタマネージャまたはリモート相関エンジンをアンインストールすることはできません。ただし、root 以外のユーザがインストールしている場合は、root 以外のユーザでアンインストールできます。

2 次の場所に移動します。

```
/opt/novell/sentinel/setup
```

3 次のコマンドを実行します。

```
./uninstall-sentinel
```

スクリプトによって、コレクタマネージャまたは相関エンジンとすべての関連データが完全に削除されるという警告が表示されます。

4 「y」と入力して、コレクタマネージャまたは相関エンジンを削除します。

スクリプトはまずサービスを停止し、その後に削除を実行します。

# 23 アンインストール後の作業

**NOTE**: Sentinel サーバをアンインストールしても、Sentinel 管理者ユーザはオペレーティングシステムから削除されません。必要に応じて、このユーザを手作業で削除する必要があります。



## 23.1 Sentinel のシステム設定の削除

Sentinel のアンインストール後も、特定のシステム設定が残ります。これらの設定は、Sentinel のクリーンインストールを実行する前に削除する必要があります。特に、Sentinel のアンインストール時にエラーが発生した場合にその必要があります。

Sentinel のシステム設定を手動でクリーンアップするには :

1. root としてログインします。
2. すべての Sentinel プロセスを停止します。
3. /opt/novell/sentinel または Sentinel ソフトウェアがインストールされていた場所の内容を削除します。
4. Sentinel 管理者オペレーティングシステムユーザ ( デフォルトでは novell) としてログインしているユーザがいないことを確認してから、ユーザ、ホームディレクトリ、およびグループを削除します。

   userdel -r novell

   groupdel novell
5. オペレーティングシステムを再起動します。

### 23.1.1 相関エンジンのアンインストールの完了

相関エンジンのアンインストールのためのアンインストールスクリプトを実行した後も、相関エンジンのアイコンは非アクティブの状態で Web インタフェースに表示されています。次の追加手順を実行して、Web インタフェースの相関エンジンを手動で削除する必要があります。

1. 管理者として Sentinel Web インタフェースにログインします。
2. ［*相関関係*］を展開してから、削除する相関エンジンを選択します。
3. ［*削除*］ボタン ( ごみ箱アイコン ) をクリックします。

### 23.1.2 コレクタマネージャのアンインストールの完了

コレクタマネージャのアンインストールのためのアンインストールスクリプトを実行した後も、コレクタマネージャのアイコンは非アクティブの状態で Web インタフェースに表示されています。次の追加手順を実行して、Web インタフェースのコレクタマネージャを手動で削除する必要があります。

1. ［*イベントソースの管理*］>［*ライブビュー*］にアクセスします。
2. 削除するコレクタマネージャを右クリックして、［*削除*］をクリックします。